

Leitfaden zur Basis-Absicherung nach IT-Grundschutz

In drei Schritten zur Informationssicherheit

Inhaltsverzeichnis

Vorwort

Cyber-Sicherheit ist ein großer, ein abstrakter Begriff. Ihn mit Leben zu füllen, beginnt jedoch schon in der kleinsten Institution. Zur Cyber-Sicherheit in Deutschland kann nicht nur der Staat beitragen, auch jedes Unternehmen – unabhängig welcher Größe – muss seinen Beitrag leisten. Mit dem IT-Grundschutz stellt das BSI seit vielen Jahren eine bewährte Methode und ein umfangreiches Angebot zur Verfügung, das in Verwaltung und Wirtschaft erfolgreich zum Einsatz kommt. Viele Behörden und große Unternehmen sind – auch aufgrund ihrer finanziellen und personellen Ausstattung – insgesamt gut in puncto Informationssicherheit aufgestellt.

Der Austausch mit kleinen und mittelständischen Unternehmern zeigt jedoch meist – noch – ein anderes Bild. Auch wenn die Awareness für Fragen der Informationssicherheit vorhanden ist, fehlt es häufig an geschultem Personal und finanziellen Spielräumen, die notwendigen Maßnahmen nachhaltig und sinnvoll umzusetzen.

Als nationale Cyber-Sicherheitsbehörde ist es unser Anspruch, die Informationssicherheit in der Digitalisierung zu gestalten und die Widerstandsfähigkeit Deutschlands gegen Cyber-Gefahren zu erhöhen. Zur Gestaltung gehört auch, praktikable und zielgruppengerechte Lösungsangebote zu machen. Der vorliegende Leitfaden „Basis-Absicherung" setzt genau hier an: Im Rahmen der gesamten IT-Grundschutz-Methodik stellt die Basis-Absicherung einen Einstieg für alle Unternehmen dar, die sich zum ersten Mal mit der Absicherung ihrer IT-Systeme und Daten befassen wollen. Der Leitfaden erläutert verständlich die erforderlichen Schritte zur Überprüfung des bestehenden Informationssicherheitsniveaus sowie schnell realisierbare Maßnahmen, die auch mit geringen finanziellen Mitteln und

wenigen Mitarbeitern umsetzbar sind. Neben technischen Aspekten werden im Sinne eines ganzheitlichen Managementsystems zur Informationssicherheit auch infrastrukturelle, organisatorische und personelle Themen betrachtet.

Ich wünsche Ihnen eine anregende Lektüre und eine gute Auseinandersetzung mit Ihren Fragen zur Informationssicherheit, vor allem aber eine erfolgreiche Umsetzung der dort beschriebenen Maßnahmen.



Ihr

Arne Schönbohm

Arne Schönbohm
Präsident des Bundesamtes für Sicherheit in der Informationstechnik

1 Einleitung

1 Einleitung

Die Herausforderungen an Verwaltung und Unternehmen, sensible Daten und Kommunikationsprozesse vor unbefugtem Zugriff zu schützen, werden zunehmend größer. Aktuelle Technologien wie Smart Home, Internet of Things sowie die weitere Digitalisierung aller Arbeits- und Lebensbereiche führen dazu, dass Institutionen jeder Größe künftig noch stärker Ressourcen in die Aufrechterhaltung der Informationssicherheit investieren müssen.

Um ein bedarfsgerechtes Sicherheitsniveau für alle Geschäftsprozesse, Informationen und IT-Systeme aufzubauen, ist mehr als die Anschaffung von Virenschutzprogrammen, Firewalls oder Datensicherungssystemen notwendig: Ein ganzheitliches Konzept bildet die Basis und den Ausgangspunkt zum Aufbau eines tragfähigen Sicherheitsmanagements. Informationssicherheitsmanagement, oder kurz IS-Management, ist der Teil des allgemeinen Risikomanagements, der die Vertraulichkeit, Integrität und Verfügbarkeit von Informationen, Geschäftsprozessen, Anwendungen und IT-Systemen gewährleisten soll. Dabei handelt es sich um einen kontinuierlichen Prozess, bei dem Strategien und Maßnahmen stetig überprüft und an veränderte Anforderungen angepasst werden.

Informationssicherheit ist nicht nur eine Frage der Technik, sie ist in erheblichem Maße von den organisatorischen und personellen Rahmenbedingungen abhängig. Der IT-Grundschutz trägt diesen Bedingungen Rechnung, indem in Veröffentlichungen sowohl technische als auch nicht-technische Sicherheitsanforderungen für typische Geschäftsbereiche, Anwendungen und Systeme auf dem Stand der Technik beschrieben werden. Im Vordergrund stehen dabei praxisnahe Sicherheitsanforderungen mit dem Ziel, die Einstiegshürde in den Sicher-

heitsprozess so niedrig wie möglich zu halten und allzu komplexe Vorgehensweisen zu vermeiden.

Leitfaden zum Einstieg in die Informationssicherheit

Der vorliegende Leitfaden zur IT-Grundschutz-Vorgehensweise „Basis-Absicherung" liefert einen kompakten und übersichtlichen Einstieg zum Aufbau eines Informationssicherheitsmanagementsystems (ISMS) in einer Institution. Ein ISMS ist ein geplantes und organisiertes Vorgehen, um ein angemessenes Sicherheitsniveau für die Informationssicherheit zu erzielen und aufrechtzuerhalten. Der Leitfaden basiert auf dem BSI-Standard 200-2 zur IT-Grundschutz-Methodik und erläutert elementare Schritte zur Überprüfung und Steigerung des Informationssicherheitsniveaus.

Im BSI-Standard 200-2 wird dargestellt, wie mit dem IT-Grundschutz ein effizientes Managementsystem für die Informationssicherheit aufgebaut werden kann. Die Vorgehensweisen nach IT-Grundschutz bieten zusammen mit dem IT-Grundschutz-Kompendium eine systematische Methodik zur Erarbeitung von Sicherheitskonzepten und praxiserprobten Sicherheitsmaßnahmen, die in zahlreichen Behörden und Unternehmen erfolgreich seit vielen Jahren eingesetzt werden.

Die Basis-Absicherung ermöglicht es, als Einstieg in den IT-Grundschutz zunächst eine breite, grundlegende Erst-Absicherung über alle Geschäftsprozesse bzw. Fachverfahren einer Institution vorzunehmen. Die Vorgehensweise ist für Institutionen empfehlenswert, auf die folgende Punkte zutreffen:

» Die Umsetzung von Informationssicherheit steht noch am Anfang, sie hat ein eher niedriges Niveau.

» Die Geschäftsprozesse haben kein deutlich erhöhtes Gefährdungspotential bezüglich der Informationssicherheit.

» Das angestrebte Sicherheitsniveau ist normal.

» Es sind keine Assets, also digitalen oder analogen Werte vorhanden, deren Diebstahl, Zerstörung oder Kompromittierung einen existenzbedrohenden Schaden für die Institution bedeutet.

» Kleinere Sicherheitsvorfälle können toleriert werden – das heißt solche, die zwar Geld kosten oder anderweitig Schaden verursachen, aber in der Summe nicht existenzbedrohend sind.

Mit der Basis-Absicherung können zeitnah die wichtigsten Sicherheitsanforderungen umgesetzt werden. Darauf aufbauend kann das Sicherheitsniveau zu einem späteren Zeitpunkt weiter erhöht werden, beispielsweise indem alle Bereiche mit der Standard-Absicherung oder kritische Geschäftsprozesse mit der Kern-Absicherung geschützt werden.

Die Basis-Absicherung stellt damit – auch und besonders – für kleine und mittelständische Unternehmen einen gut realisierbaren Einstieg in eine gelebte Praxis zur Informationssicherheit dar. Mit einem verhältnismäßig geringen Aufwand ist sehr schnell eine grundlegende Erst-Absicherung erzielbar.

Entscheidung für die Basis-Absicherung

Die IT-Grundschutz-Methodik stellt neben der Basis-Absicherung zwei weitere Vorgehensweisen zur Verfügung, die abhängig von den individuellen Sicherheitsanforderungen einer Institution eingesetzt werden können. Verantwortliche für die

Informationssicherheit können daher zwischen der Basis-, der Standard- und der Kern-Absicherung wählen.

Mit der Basis-Absicherung kann ein erster Einstieg in ein Sicherheitsmanagement vollzogen werden, um schnellstmöglich die größten Risiken zu senken. Im Vergleich dazu dient die Kern-Absicherung dem Schutz elementarer Geschäftsprozesse und Ressourcen.

Wenn die Basis-Absicherung in einer Institution erfolgreich umgesetzt wurde, kann und sollte als nächster Schritt für eine solide Informationssicherheit mit der Standard- oder Kern-Absicherung fortgefahren werden. Im besten Fall wird mit der Zeit eine vollständige Standard-Absicherung auf Basis des BSI-Standards 200-2 umgesetzt, damit ein dem Schutzbedarf angemessenes Sicherheitsniveau erreicht wird.

Zielgruppe

Grundsätzlich richtet sich der Leitfaden Basis-Absicherung an diejenigen Personen in Unternehmen, die Informationssicherheit umsetzen. Typischerweise sind das Informationssicherheitsbeauftragte (ISB). Bei kleineren Institutionen, in denen der Bereich Informationssicherheit bislang (noch) nicht so professionell aufgestellt ist, können auch andere Mitarbeiter zunächst diese Aufgabe übernehmen. Geeignet sind beispielsweise Mitarbeiter aus den Bereichen Finanzen und Controlling, IT-Betrieb oder der betriebliche Datenschutzbeauftragte, allerdings aufgrund ihrer originären Aufgaben und möglicher Rollenkonflikte nur mit Einschränkungen.

Basis-Absicherung: Mehrwert für die Informationssicherheit

Der Leitfaden Basis-Absicherung gibt Verantwortlichen das notwendige Rüstzeug an die Hand, um das Niveau der Informationssicherheit in einer Institution zu überprüfen, Schwachstellen zu identifizieren und mit geeigneten Maßnahmen zu verbessern. Die Basis-Absicherung ermöglicht dabei ein überschaubares und sehr praktikables Vorgehen für eine Erstabsicherung. Mit dem ganzheitlichen Ansatz der IT-Grundschutz-Methodik, bei der neben technischen auch infrastrukturelle, organisatorische und personelle Aspekte betrachtet werden, können geschäftlich relevante Informationen und Daten vor Missbrauch und fremdem Zugriff geschützt werden.

2 Informationssicherheitsmanagement mit IT-Grundschutz

2 Informationssicherheitsmanagement mit IT-Grundschutz

Im BSI-Standard 200-2 wird dargestellt, wie ein effizientes Managementsystem für die Informationssicherheit aufgebaut und wie das IT-Grundschutz-Kompendium im Rahmen dieser Aufgabe verwendet werden kann. Die Vorgehensweisen nach IT-Grundschutz in Kombination mit den Bausteinen des IT-Grundschutz-Kompendiums bieten eine systematische Methodik zur Erarbeitung von Sicherheitskonzepten und praxiserprobten Sicherheitsmaßnahmen, die in zahlreichen Behörden und Unternehmen erfolgreich eingesetzt werden. Der vorliegende Leitfaden erläutert unter Anwendung der Basis-Absicherung aus dem BSI-Standard 200-2 schematisch den Prozess zur Etablierung eines ISMS und wie dieser fortgeführt werden kann.

Übersicht über den Informationssicherheitsprozess

Für die Gestaltung des Sicherheitsprozesses ist ein systematisches Vorgehen erforderlich, damit ein angemessenes Sicherheitsniveau erreicht werden kann.

Die ganzheitliche Umsetzung von Informationssicherheit in einem einzelnen großen Schritt hat sich schon oft als ein zu ehrgeiziges Ziel erwiesen. Viele kleine Schritte und ein langfristiger, kontinuierlicher angelegter Prozess sind oft Erfolg versprechender.

Auch hohe Investitionskosten zu Beginn sind meist nicht erforderlich. So kann es besser sein, zunächst nur in ausgewählten Bereichen die dringend erforderlichen Sicherheitsvorkehrungen umzusetzen. Dieser Ansatz entspricht der Basis-Absicherung. Sind die dringendsten Sicherheitsfragen geklärt, können im Anschluss alle weiteren Aspekte in der Gesamtorganisation überprüft und verbessert werden.

1. Initiierung des Sicherheitsprozesses
✓ Verantwortung übernehmen / der ISB als zentrale Rolle
✓ Geltungsbereich: der Informationsverbund
✓ Sicherheitsziele festlegen und Leitlinie erstellen

2. Organisation des Sicherheitsprozesses
✓ Aufbau einer Organisation zur Informationssicherheit
✓ Integration in bestehende Abläufe und Prozesse
✓ Konzeption und Planung des Sicherheitsprozesses

3. Durchführung des Sicherheitsprozesses
✓ Auswahl und Priorisierung der Bausteine (Modellierung)
✓ IT-Grundschutz-Check
✓ Umsetzung der Sicherheitskonzeption

Abbildung 1: In drei Schritten zur Informationssicherheit

Der vorliegende Leitfaden zeigt, wie die Basis-Absicherung in drei Schritten umgesetzt werden kann. Die Schritte orientieren sich dabei stark an den Phasen des Sicherheitsprozesses gemäß der IT-Grundschutz-Methodik.

Einige dieser Phasen können parallel durchgeführt werden, zum Beispiel können Konzeption und Planung des Sicherheitsprozesses gleichzeitig zur Etablierung der Informationssicher-

heitsorganisation erfolgen. In diesem Fall müssen die vorgezogenen Phasen mit den neuen Ergebnissen zeitnah aktualisiert werden.

Im Folgenden wird eine kurze Darstellung über die Schritte des Sicherheitsprozesses gegeben.

1. Initiierung des Sicherheitsprozesses

Die Leitungsebene muss den Sicherheitsprozess initiieren, steuern und kontrollieren. Hierfür sind einerseits strategische Leitaussagen zur Informationssicherheit und andererseits organisatorische Rahmenbedingungen erforderlich. Der Informationssicherheitsbeauftragte (ISB) spielt die zentrale Rolle in diesem Prozess.

Eine wesentliche Grundlage für die Ausgestaltung des Sicherheitsprozesses ist die Leitlinie zur Informationssicherheit. Sie beschreibt, für welchen Geltungsbereich die Institution welche Sicherheitsziele und welches Sicherheitsniveau anstrebt, was die Motivation hierfür ist und mit welchen Maßnahmen und mit welchen Strukturen dies erreicht werden soll.

2. Organisation des Sicherheitsprozesses

Für das Informationssicherheitsmanagement muss eine für Größe und Art der Institution geeignete Organisationsstruktur aufgebaut werden. Hierzu müssen Schnittstellen, Kommunikationswege und Prozesse zur Zusammenarbeit festgelegt werden. Bei sehr kleinen Unternehmen kann dies in einem möglichst überschaubaren Rahmen erfolgen.

3. Durchführung des Sicherheitsprozesses

Nachdem ein Informationssicherheitsprozess initiiert und die Sicherheitsleitlinie und Informationssicherheitsorganisation definiert wurden, kann im nächsten Schritt die Sicherheitskonzeption für die Institution erstellt werden. Als Grundlage gibt es in den Bausteinen des IT-Grundschutz-Kompendiums für typische Komponenten von Geschäftsprozessen, Anwendungen, IT-Systeme und weitere Objekte entsprechende Sicherheitsanforderungen gemäß dem Stand der Technik. Diese sind thematisch strukturiert und setzen modular aufeinander auf.

Bei der IT-Grundschutz-Methodik reduziert sich der Analyseaufwand auf einen Soll-Ist-Vergleich zwischen den Sicherheitsanforderungen aus den relevanten Bausteinen und den in der Institution bereits realisierten Maßnahmen. Dabei festgestellte fehlende oder nur unzureichend erfüllte Anforderungen zeigen die Sicherheitsdefizite auf, die es durch die konsequente Umsetzung von abgeleiteten Maßnahmen zu beheben gilt.

Aufrechterhaltung und Verbesserung der Informationssicherheit

Ziel des Sicherheitsmanagements ist es, ein angestrebtes Sicherheitsniveau zu erreichen und dieses dauerhaft aufrechtzuerhalten sowie bestenfalls stetig zu verbessern. Daher müssen der Prozess selbst und die Organisationsstrukturen für Informationssicherheit regelmäßig daraufhin überprüft werden, ob sie angemessen, wirksam und effizient sind. Dasselbe gilt für die gewählten Maßnahmen. Nach Abschluss einer initialen Basis-Absicherung sollte die Vorgehensweise ergänzt oder erweitert werden, beispielsweise von Basis- auf Standard-Absicherung oder durch Anwendung der Kern-Absicherung.

3 Erstellung einer Sicherheitskonzeption nach der Basis-Absicherung

3 Erstellung einer Sicherheitskonzeption nach der Basis-Absicherung

Dieses Kapitel beschreibt im Detail, wie eine Sicherheitskonzeption in drei Schritten nach der Basis-Absicherung umgesetzt werden kann.

3.1 Initiierung des Sicherheitsprozesses

In diesem Kapitel werden die ersten Schritte zur Umsetzung einer Basis-Absicherung in einer Institution beschrieben. Die Verantwortung tragen dabei die Leitung oder Geschäftsführung. Zudem nimmt der Informationssicherheitsbeauftragte (ISB) eine zentrale Rolle ein, schließlich geht es bereits zu diesem Zeitpunkt um die Festlegung der Sicherheitsziele in Form einer Leitlinie.

3.1.1 Management-Entscheidung: Verantwortung der Leitungsebene

Die oberste Leitungsebene ist dafür verantwortlich, dass alle Geschäftsbereiche reibungslos und ordnungsgemäß funktionieren und Risiken frühzeitig erkannt und minimiert werden. Mit der zunehmenden Abhängigkeit der Geschäftsprozesse von der Informationsverarbeitung steigen damit auch die Anforderungen daran, dass Informationssicherheit nach innen und außen gewährleistet ist.

Die Leitung muss den Sicherheitsprozess initiieren, steuern und kontrollieren. Sie entscheidet über den Umgang mit Risiken und stellt Ressourcen zur Verfügung. Die Verantwortung für die Informationssicherheit verbleibt dort. Die operative Aufgabe „Informationssicherheit“ wird allerdings üblicherweise an einen Informationssicherheitsbeauftragten delegiert.

In der Einstiegsphase in den Sicherheitsprozess ist meist noch keine Sicherheitsorganisation aufgebaut und häufig auch noch nicht der spätere ISB benannt. Für die Initiierung des Sicherheitsprozesses muss aber zumindest ein Verantwortlicher für Informationssicherheit benannt werden, der die ersten Schritte zur Konzeption und Planung durchführt.

Für die Verantwortlichen ist es empfehlenswert, die oberste Leitungsebene stets über mögliche Risiken und Konsequenzen aufgrund fehlender Informationssicherheit aufzuklären. Nach einem Sicherheitsvorfall muss die Geschäftsführung oder Behördenleitung zeitnah über mögliche Risiken unterrichtet werden. Auf der anderen Seite muss die Leitung sicherstellen, dass ihr alle entscheidungsrelevanten Informationen rechtzeitig vorliegen.

Auf einen Blick: Sicherheitsrelevante Themen für die Leitungsebene

- » Sicherheitsrisiken für die Institution und deren Informationen
- » Auswirkungen und Kosten im Schadensfall
- » Auswirkungen von Sicherheitsvorfällen auf kritische Geschäftsprozesse
- » Sicherheitsanforderungen, die sich aus gesetzlichen und vertraglichen Vorgaben ergeben
- » die für eine Branche typischen Vorgehensweisen zur Informationssicherheit
- » der aktuelle Stand der Informationssicherheit in der Institution mit abgeleiteten Handlungsempfehlungen

Die Leitungsebene trägt die Verantwortung für die Erreichung der Sicherheitsziele, die operative Umsetzung und Steuerung des Sicherheitsprozesses obliegt einem verantwortlichen ISB. Alle Beschäftigten in einer Institution müssen ihren Teil dazu beitragen, die Sicherheitsziele zu erreichen.

Die Leitungsebene muss sich vor allem dafür einsetzen, dass Informationssicherheit in alle relevanten Geschäftsprozesse bzw. Fachverfahren und Projekte integriert wird. Der ISB braucht hierbei erfahrungsgemäß die volle Unterstützung der Behörden- oder Unternehmensleitung, um von den jeweiligen Fachverantwortlichen eingebunden zu werden.

Die Leitungsebene muss die Ziele sowohl für das Informationssicherheitsmanagement als auch für alle anderen Bereiche so setzen, dass das angestrebte Sicherheitsniveau in allen Bereichen mit den bereitgestellten Ressourcen (Personal, Zeit, Finanzmittel) erreichbar ist.

Auf einen Blick: Verantwortung durch die Leitungsebene

- Die Leitungsebene trägt die Gesamtverantwortung für Informationssicherheit.
- Die Leitungsebene muss jederzeit über mögliche Risiken und Konsequenzen für die Informationssicherheit informiert sein.
- Die Leitungsebene initiiert den Informationssicherheitsprozess innerhalb der Institution und benennt einen Verantwortlichen Informationssicherheitsbeauftragten (ISB).
- Die Leitungsebene unterstützt den ISB vollständig und stellt ausreichende Ressourcen bereit, um die gesetzten Ziele erreichen zu können.

3.1.2 Zentrale Rolle: Der Informationssicherheitsbeauftragte (ISB)

In einer Institution muss es einen Ansprechpartner für alle Aspekte rund um das Thema Informationssicherheit geben. Nur ein zentraler Ansprechpartner kann ein gängiges Problem lösen: Im geschäftlichen Alltag werden Aspekte der Informationssicherheit häufig vernachlässigt, sie gehen in manchen Institutionen schlichtweg unter. Dadurch besteht bei fehlender oder unklarer Aufteilung der Zuständigkeit die Gefahr, dass

Informationssicherheit grundsätzlich zu einem „Problem anderer Leute“ wird.

Die Rolle des Informationssicherheitsbeauftragten setzt hier an. Der ISB koordiniert die Aufgabe „Informationssicherheit“, identifiziert Schwachstellen und arbeitet daran, das Sicherheitsniveau zu erhöhen. Für die Funktion gibt es in Wirtschaft und Verwaltung diverse Bezeichnungen: Häufige Titel sind auch Chief Information Security Officer (CISO) oder Informationssicherheitsmanager (ISM). In einigen Institutionen wird auch die Bezeichnung IT-Sicherheitsbeauftragter (IT-SiBe) verwendet. ISB ist hier jedoch die treffendere Bezeichnung. Sie verdeutlicht, dass der Verantwortliche sich nicht nur um die Absicherung IT-bezogener Aspekte kümmert, sondern um den Schutz aller Arten von Informationen.

Es ist abhängig von der Art und Größe der Institution, ob oder wie viele weitere Mitarbeiter Sicherheitsaufgaben übernehmen.

Zuständigkeiten und Aufgaben

Der ISB ist zuständig für die Wahrnehmung aller Belange der Informationssicherheit innerhalb der Institution. Seine Hauptaufgabe besteht darin, die Behörden- bzw. Unternehmensleitung bei deren Aufgabenwahrnehmung bezüglich der Informationssicherheit zu beraten und sie bei der Umsetzung zu unterstützen.

Der ISB ist bei allen größeren Projekten, die deutliche Auswirkungen auf die Informationsverarbeitung haben könnten, zu beteiligen, um die Beachtung von Sicherheitsaspekten in den verschiedenen Projektphasen zu gewährleisten. So sollte der ISB bei der Planung und Einführung neuer Anwendungen und IT-Systeme ebenso beteiligt sein wie bei wesentlichen Ände-

rungen der Infrastruktur oder der Auslagerung von Geschäftsprozessen (Outsourcing). Auch Produktionsanlagen und andere Geräte mit IT- oder Internet-Funktionalität dürfen nicht vergessen werden. Zur Erfüllung dieser Aufgaben ist es wünschenswert, dass der Informationssicherheitsbeauftragte über Wissen und Erfahrung in den Gebieten Informationssicherheit und IT verfügt. Ebenso sollte er Kenntnisse über die Geschäftsprozesse der Institution mitbringen.

Personalunion mit dem Datenschutzbeauftragten

Eine häufige Frage ist, ob die Position des Informationssicherheitsbeauftragten gleichzeitig vom Datenschutzbeauftragten wahrgenommen werden kann. Die beiden Rollen schließen sich nicht grundsätzlich aus, es sind allerdings einige Aspekte im Vorfeld zu klären:

» Die Schnittstellen zwischen den beiden Rollen sollten klar definiert und dokumentiert werden.

» Für beide Rollen sollte es direkte Berichtswege zur Leitungsebene geben.

» Es muss sichergestellt sein, dass es ausreichend Ressourcen für die Wahrnehmung beider Rollen gibt. Gegebenenfalls muss durch entsprechendes Personal unterstützt werden.

Es darf nicht vergessen werden, dass auch der Informationssicherheitsbeauftragte einen qualifizierten Vertreter benötigt.

Generell ist empfehlenswert, für beide Themen – Informationssicherheit und Datenschutz – jeweils einen verantwortlichen Ansprechpartner zu benennen. Der Datenschutzbeauftragte sollte vergleichbar dem ISB alle Aspekte des Datenschutzes

innerhalb der Institution begleiten und angemessene Kontrollmechanismen einführen. In ihren Funktionen arbeiten beide eng zusammen und berichten an die Leitungsebene.

Auf einen Blick: Zuständigkeiten und Aufgaben des ISB

» Informationssicherheitsprozess steuern und bei allen damit zusammenhängenden Aufgaben mitwirken

» die Leitungsebene bei der Erstellung der Leitlinie zur Informationssicherheit unterstützen

» die Erstellung des Sicherheitskonzepts, des Notfallvorsorgekonzepts und Sicherheitsrichtlinien koordinieren sowie weitere Richtlinien und Regelungen zur Informationssicherheit erlassen

» die Realisierung von Sicherheitsmaßnahmen initiieren und überprüfen

» der Leitungsebene über den Status quo der Informationssicherheit berichten

» sicherheitsrelevante Projekte koordinieren

» Sicherheitsvorfälle untersuchen

» Sensibilisierungs- und Schulungsmaßnahmen zur Informationssicherheit initiieren und koordinieren

3.1.3 Geltungsbereich für die Sicherheitskonzeption: der Informationsverbund

Der Bereich der Institution, für den die Basis-Absicherung umgesetzt werden soll, wird Geltungsbereich oder „Informationsverbund" genannt. Ein Informationsverbund umfasst die Gesamtheit von infrastrukturellen, organisatorischen, personellen und technischen Komponenten, die der Aufgabenerfüllung in einem bestimmten Anwendungsbereich der Informationsverarbeitung dienen. Ein Informationsverbund kann dabei die gesamte Informationsverarbeitung einer Institution oder auch einzelne Bereiche umfassen, die durch organisatorische bzw. technische Strukturen (z. B. Abteilungsnetz) oder gemeinsame Geschäftsprozesse bzw. Anwendungen (z. B. Personalinformationssystem) gegliedert sind. Für die Anwendung der Basis-Absicherung muss festgelegt werden, wie der zu schützende Informationsverbund aussehen soll. Wichtig ist, dass die betrachteten Geschäftsaufgaben und -prozesse in dem Geltungsbereich komplett enthalten sind. Insbesondere bei größeren Institutionen ist es keine triviale Aufgabe, den Geltungsbereich festzulegen. Eine Orientierung nach Verantwortlichkeiten kann bei der Festlegung des Geltungsbereichs behilflich sein. Bei der Basis-Absicherung umfasst der Geltungsbereich in der Regel die gesamte Institution.

Es sollten nicht nur technische, sondern auch organisatorische Aspekte bei der Abgrenzung des Geltungsbereichs berücksichtigt werden, damit die Verantwortlichkeiten und die Zuständigkeiten eindeutig festgelegt werden können. In jedem Fall sollte klar sein, welche Informationen, Fachaufgaben oder Geschäftsprozesse in der Sicherheitskonzeption explizit betrachtet werden.

Bei der Abgrenzung des Informationsverbundes müssen folgende Faktoren berücksichtigt werden:

Der Geltungsbereich sollte möglichst alle Bereiche, Aspekte und Komponenten umfassen, die zur Unterstützung der Fachaufgaben, Geschäftsprozesse oder Organisationseinheiten dienen und deren Verwaltung innerhalb der Institution stattfindet.

Wenn dies nicht möglich ist, weil Teile der betrachteten Fachaufgaben oder Geschäftsprozesse organisatorisch von externen Partnern abhängig sind, beispielsweise im Rahmen von Outsourcing, sollten die Schnittstellen klar definiert werden, damit dies im Rahmen der Sicherheitskonzeption berücksichtigt werden kann.

Ein wichtiger Aspekt: Outsourcing

Die Auslagerung von Geschäfts- und unterstützenden Prozessen, wie beispielsweise dem IT-Betrieb, wird von vielen Experten weiterhin recht kritisch gesehen. In kleineren Institutionen kann ein gut geplantes Outsourcing-Projekt dennoch dazu beitragen, das Niveau der Informationssicherheit anzuheben. Dies trifft besonders dann zu, wenn Outsourcing-Lösungen oder der Einkauf externer Dienstleistungen dazu genutzt werden, um in der Institution fehlendes Know-how auszugleichen. Damit Outsourcing-Lösungen sich positiv auf die Informationssicherheit auswirken können, müssen allerdings einige Regeln beachtet werden: Bevor Geschäftsprozesse ausgelagert werden können, muss zunächst geklärt werden, ob aus Sicherheitssichtgründen etwas dagegen spricht. Dies könnte zum Beispiel ein nicht ausreichend garantierter Schutz von vertraulichen Daten sein.

Sobald eine Entscheidung für eine Outsourcing-Lösung getroffen wurde, müssen die wesentlichen Sicherheitsanforderungen für das Vorhaben festgelegt werden. Diese bilden unter anderem die Basis für die Auswahl eines Outsourcing-Dienstleisters.

Bei der Auswahl sind Nachweise über die Informationssicherheit in der Institution und die Qualifikationen der Mitarbeiter einzuholen. Dabei können Zertifikate wie IT-Grundschutz bzw. ISO 27001 hilfreiche Indikatoren für ein gewisses Sicherheitsniveau sein.

Bei der Vertragsgestaltung mit einem Outsourcing-Dienstleister müssen die Sicherheitsanforderungen und die Kriterien zu Servicequalität und Sicherheit möglichst detailliert beschrieben werden. Im Vertrag müssen zudem Auskunfts-, Mitwirkungs- und Revisionspflichten geregelt sein.

Auftraggeber und Outsourcing-Dienstleister müssen darüber hinaus ein detailliertes Sicherheitskonzept inklusive eines Notfallvorsorgekonzepts abstimmen. Bei der Übertragung der Aufgaben müssen Verantwortlichkeiten festgelegt und auf beiden Seiten Ansprechpartner benannt werden. Der Auftraggeber muss außerdem auch während des Outsourcing-Vorhabens regelmäßige Kontrollen zur Aufrechterhaltung der Informationssicherheit beim Dienstleister durchführen (lassen). Vor Abschluss eines Outsourcing-Projekts sollten die Eigentumsrechte an der Hard- und Software sowie die Rückgabe der Datenbestände vom Dienstleister geklärt sein.

Informationssicherheit ist ein elementares Thema, das frühzeitig bei der Auswahl von möglichem Outsourcing-Dienstleistern angesprochen werden sollte. In mehrstufig angelegten Verhandlungen mit den unterschiedlichen Anbietern können interne Risikobewertungen die Auswahl erleichtern. Allerdings wird sich nicht jedes Sicherheitsmerkmal aus dem Pflichtenheft zu einem angemessenen Preis realisieren lassen. Weitere Informationen zum Thema Outsourcing sind im IT-Grundschutz-Kompendium insbesondere im Baustein OPS.2 „Betrieb von Dritten“ zu finden.

Auf einen Blick: Definition des Informationsverbundes

» Festlegen, welche kritischen Geschäftsprozesse, Fachaufgaben oder Teile der Institution der Geltungsbereich beinhalten soll.

» Den Geltungsbereich eindeutig abgrenzen.

» Schnittstellen zu externen Partnern beschreiben.

3.1.4 Erstellung einer Leitlinie zur Informationssicherheit

Die Leitlinie zur Informationssicherheit dient als Ausgangspunkt für die geplante Auseinandersetzung mit den Anforderungen an Informationssicherheit in der eigenen Institution. In ihr sind allgemeinverständlich die Ziele und Mittel zur Erreichung eines höheren Sicherheitsniveaus festzuschreiben. Neben den angestrebten Informationssicherheitszielen enthält sie auch die grundlegende Sicherheitsstrategie. Die Leitlinie beschreibt über die Sicherheitsziele auch das angestrebte Sicherheitsniveau in einer Behörde oder einem Unternehmen. Sie ist somit Anspruch und Aussage zugleich, dass ein bestimmtes Sicherheitsniveau auf allen Ebenen der Institution erreicht werden soll.

Verantwortung der Institutionsleitung für die Sicherheitsleitlinie

Mit der Leitlinie zur Informationssicherheit wird dokumentiert, welche strategische Position die Institutionsleitung zur Erreichung der Informationssicherheitsziele vorgibt.

Da die Sicherheitsleitlinie ein zentrales Strategiepapier für die Informationssicherheit einer Institution darstellt, muss sie so

formuliert und aufbereitet sein, dass sich alle Adressaten mit ihr identifizieren können. Der ISB sollte daher an der Erstellung der Leitlinie möglichst viele Bereiche beteiligen. Folgende Organisationseinheiten können zum Beispiel einbezogen werden: Fachverantwortliche für wichtige Anwendungen, IT-Betrieb, Sicherheit (Informations-, IT- und Infrastruktur-Sicherheit), Datenschutzbeauftragter, Produktion und Fertigung, Personalabteilung, Personalvertretung, Revision, Vertreter für Finanzfragen oder die Rechtsabteilung.

Formulierung von allgemeinen Informationssicherheitszielen

Zu Beginn jedes Sicherheitsprozesses sollten die Informationssicherheitsziele sorgfältig gemäß der konkreten Anforderungen bestimmt werden. Aus diesen werden bei der Erstellung der Sicherheitsleitlinie und später bei der Erstellung des Sicherheitskonzeptes und bei der Ausgestaltung der Informationssicherheitsorganisation konkrete Sicherheitsanforderungen an den Umgang mit Informationen abgeleitet.

Um die Sicherheitsziele definieren zu können, sollte zunächst abgeschätzt werden, welche Geschäftsprozesse bzw. Fachverfahren und Informationen für die Aufgabenerfüllung notwendig sind und welcher Wert diesen beigemessen wird. Dabei ist es wichtig, klarzustellen, wie stark die Aufgabenerfüllung innerhalb der Institution von den Grundwerten Vertraulichkeit, Integrität und Verfügbarkeit von Informationen und von der eingesetzten IT abhängt. Diese Aussagen werden im Lauf des Sicherheitsprozesses bei der Wahl der Sicherheitsmaßnahmen und Strategien eine entscheidende Rolle spielen.

An diesem Prozessschritt ist keine detaillierte Analyse des Informationsverbundes erforderlich. Als Ergebnis sollte eine

Aussage möglich sein, welche Werte oder Prozesse für die Institution besonders wichtig sind, sowie die Gründe dafür.

Auf einen Blick: Beispiele für Sicherheitsziele

» hohe Verlässlichkeit des Handelns, auch in Bezug auf den Umgang mit Informationen (Verfügbarkeit, Integrität, Vertraulichkeit)

» Gewährleistung der guten Reputation der Institution in der Öffentlichkeit

» Erhaltung der in Technik, Informationen, Arbeitsprozesse und Wissen investierten Werte

» Sicherung der hohen, möglicherweise unwiederbringlichen Werte der verarbeiteten Informationen

» Gewährleistung der aus gesetzlichen Vorgaben resultierenden Anforderungen

» Schutz von natürlichen Personen hinsichtlich ihrer körperlichen und geistigen Unversehrtheit

Inhalt der Sicherheitsleitlinie

Die Sicherheitsleitlinie sollte kurz und bündig formuliert sein. Mehr als zehn Seiten sind selten erforderlich. Die zwischen ISB und Leitung abgestimmte, finale Version der Leitlinie sollte allen Mitarbeitern zur Kenntnis gegeben und an einer zentralen Stelle, zum Beispiel im Intranet, veröffentlicht werden. An der Aufgabe „Informationssicherheit" muss schließlich jeder Mitarbeiter aktiv mitwirken. Die Sicherheitsleitlinie liefert hier einen

wichtigen Beitrag zur Steigerung der Awareness zur Informationssicherheit in einer Institution.

In der folgenden Übersicht sind die grundlegenden Inhalte für eine Sicherheitsleitlinie dargestellt:

» Stellenwert der Informationssicherheit und Bedeutung der wesentlichen Informationen, Geschäftsprozesse und der IT für die Aufgabenerfüllung

» Bezug der Informationssicherheitsziele zu den Geschäftszielen oder Aufgaben der Institution

» Sicherheitsziele und die Kernelemente der Sicherheitsstrategie für die Geschäftsprozesse und die eingesetzte IT

» Zusicherung, dass die Sicherheitsleitlinie von der Institutionsleitung durchgesetzt wird

» Leitaussagen zur Erfolgskontrolle

» Beschreibung der geplanten Organisationsstruktur

» Aufgaben und Zuständigkeiten im Sicherheitsprozess sollten aufgezeigt werden

» Programme zur Förderung der Informationssicherheit durch Schulungs- und Sensibilisierungsmaßnahmen können angekündigt werden

» wichtige Gefährdungen, relevante gesetzliche Regelungen etc. können eingangs skizziert werden.

Aufgrund sich verändernder Geschäftsziele und -prozesse ist es ratsam, die Sicherheitslinie regelmäßig bzw. anlassbezogen auf den Prüfstand zu stellen und zu aktualisieren.

Auf einen Blick: Erstellung einer Sicherheitsleitlinie

» zu beteiligende Organisationseinheiten für die Sicherheitsleitlinie identifizieren

» gemeinsam Geltungsbereich und Inhalte festlegen

» Inkraftsetzung der Sicherheitsleitlinie durch die Leitungsebene veranlassen

» Sicherheitsleitlinie bekannt geben

» Sicherheitsleitlinie regelmäßig überprüfen und gegebenenfalls aktualisieren

3.2 Organisation des Sicherheitsprozesses

Um ein angemessenes und ausreichendes Niveau der Informationssicherheit in der Institution zu erzielen bzw. dieses aufrechtzuerhalten, sind ein geplantes Vorgehen und eine adäquate Organisationsstruktur unerlässlich. Darüber hinaus ist es notwendig, Sicherheitsziele und eine Strategie zur Erreichung dieser Ziele zu definieren sowie letztendlich einen kontinuierlichen Sicherheitsprozess zur Aufrechterhaltung des einmal erreichten Sicherheitsniveaus einzurichten.

3.2.1 Aufbau einer Organisation zur Informationssicherheit

Das angestrebte Sicherheitsniveau kann nur erreicht werden, wenn die Anforderungen aus dem Informationssicherheitsprozess im gesamten Geltungsbereich der Leitlinie gleichmäßig umgesetzt werden. Diese Bedingung macht es notwendig, Rollen innerhalb der Institution festzulegen, die die Umsetzung des Prozesses verantwortlich übernehmen. Die Mitarbeiter sollten in allen Fragen der Informationstechnik sowie Informationssicherheit angemessen qualifiziert sein. Nur so kann gewährleistet werden, dass alle wichtigen Aspekte berücksichtigt und sämtliche Aufgaben bewältigt werden.

Die Aufbauorganisation, die zur Förderung und Durchsetzung des Informationssicherheitsprozesses erforderlich ist, wird als Informationssicherheitsorganisation oder kurz IS-Organisation bezeichnet. Die Zusammensetzung einer IS-Organisation hängt von der Größe, Beschaffenheit und Struktur der jeweiligen Institution ab. Als zentraler Ansprechpartner für die Koordination, Verwaltung und Kommunikation des Prozesses Informationssicherheit sollte grundsätzlich der ISB benannt sein. In größeren Institutionen gibt es darüber hinaus häufig weitere Mitarbeiter, die Teilaufgaben im Bereich der Informationssicherheit übernehmen.

Die Rollen sollten einen direkten Zugang zur Geschäftsführung haben und dieser unmittelbar unterstellt sein. Auf der Leitungsebene sollte die Aufgabe Informationssicherheit von einem verantwortlichen Manager übernommen werden, an den der ISB berichtet.

Unabhängig davon, wie eine optimale Struktur für die eigene IS-Organisation zu gestalten ist, sind die folgenden Grundregeln dabei unbedingt zu beachten.

Grundregeln bei der Definition von Rollen im Informationssicherheitsmanagement

» Die Gesamtverantwortung für die ordnungsgemäße und sichere Aufgabenerfüllung obliegt der Leitungsebene.

» Es ist mindestens eine Person zum ISB zu ernennen, die den Informationssicherheitsprozess koordiniert und steuert.

» Alle Mitarbeiter sind gleichermaßen sowohl für ihre originären Aufgaben als auch für die Aufrechterhaltung der Informationssicherheit an ihrem Arbeitsplatz und in ihrer Umgebung verantwortlich.

» Informationssicherheit muss in Abläufe und Prozesse innerhalb der gesamten Institution integriert und Ansprechpartner müssen festgelegt werden. Ziel ist es, dass bei allen strategischen Entscheidungen die notwendigen Sicherheitsaspekte frühzeitig berücksichtigt werden.

Da Risiken für die Informationssicherheit ebenso wie IT-Risiken zu den wichtigsten Gefährdungen für das operationelle Tagesgeschäft gehören, sollten die Methoden zum Informationssicherheitsmanagement mit den bereits vorhandenen zum Umgang mit Risiken in anderen Bereichen abgestimmt werden. Detailliertere Informationen hierzu finden sich auch im BSI-Standard 200-3 „Risikoanalyse auf der Basis von IT-Grundschutz“.

Aufbau der Informationssicherheitsorganisation

Abhängig von der Größe einer Institution gibt es unterschiedliche Möglichkeiten zur Ausgestaltung einer Aufbauorganisation für ein Informationssicherheitsmanagement. Die folgende Abbildung zeigt den Aufbau einer IS-Organisation in einer kleinen Institution. Hier steht der ISB in engem Austausch mit der Leitung, den jeweiligen Fachverantwortlichen und dem betrieblichen Datenschutzbeauftragten (bDSB). Der ISB fungiert als Schnittstelle zwischen den anderen Beteiligten. Die IS-Leitlinien und Vorgaben sind unter der Leitung des ISB mit den anderen Verantwortlichen abgestimmt und veröffentlicht worden. Sie bilden die Grundlage für den Umgang aller Beschäftigten mit den Themen der Informationssicherheit.

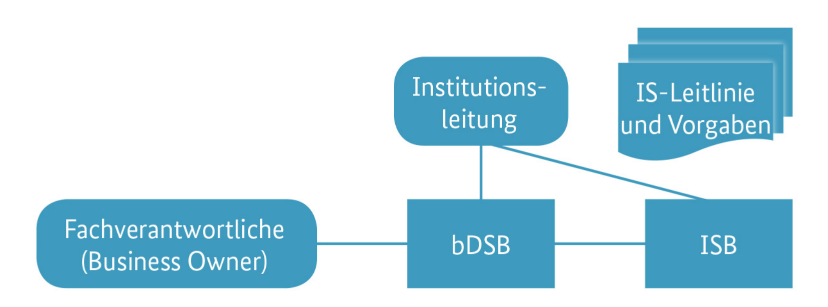


Abbildung 2: Aufbau der IS-Organisation in einer kleinen Institution

Zusammenspiel mit anderen Organisationseinheiten und Managementdisziplinen

In den meisten Institutionen gibt es neben dem Informationssicherheitsmanagement auch andere Bereiche, die Aufgaben zur Informationssicherheit wahrnehmen oder mit vergleichbaren Themen betraut sind. Ein koordiniertes Vorgehen und die Festlegung von Schnittstellen sind unerlässlich, zumal diese Bereiche häufig als getrennte Disziplinen und teilweise auch in

anderen Organisationseinheiten organisiert sind. Gemeinsam ist ihnen, dass sie das Ziel verfolgen, Werte der Institution zu schützen. Beispielsweise gehören hierzu neben dem Informationssicherheitsmanagement die Themenfelder Datenschutz, Objektschutz, Personenschutz, Geheimschutz, Notfallmanagement oder Risikomanagement. In Institutionen mit einem Produktionsbereich ist darüber hinaus die Zusammenarbeit mit den Verantwortlichen für die Produkt- und Anlagensicherheit wichtig.

Zusammenarbeit mit dem IT-Betrieb

Viele Teilaufgaben des Sicherheitsmanagements hängen unmittelbar mit Aufgaben des IT-Betriebs zusammen. Der ISB erstellt Vorgaben für den sicheren Betrieb von IT-Systemen und Netzen, der IT-Betrieb muss diese umsetzen. Daher müssen das Sicherheitsmanagement und der IT-Betrieb eng zusammenarbeiten und sich regelmäßig über Vorgehensweisen, aktuelle Gefährdungen und neue Sicherheitsanforderungen austauschen. In größeren Institutionen kann es daher sinnvoll sein, einen dedizierten Ansprechpartner des ISB im IT-Betrieb zu ernennen.

Auf einen Blick: Organisation des Sicherheitsprozesses

» Rollen für die Gestaltung des Informationssicherheitsprozesses festlegen

» Aufgaben und Verantwortungsbereiche den Rollen zuordnen

» Personelle Ausstattung der Rollen festlegen

» IS-Organisation dokumentieren

» Informationssicherheitsmanagement in die Abläufe und Prozesse integrieren

3.2.2 Konzeption und Planung des Sicherheitsprozesses

Für die weiteren Schritte im Sicherheitsprozess sollten alle relevanten Rahmenbedingungen identifiziert werden. Dafür sollten die wichtigsten Geschäftsprozesse und Fachaufgaben sowie deren Bedarf an Informationssicherheit ermittelt werden.

Die Ermittlung der Rahmenbedingungen ist eine wichtige Grundlage für die weiteren Betrachtungen zur Informationssicherheit: Bereits an dieser Prozessstelle kann auffallen, wenn relevante Informationen fehlen, und eine erste Einschätzung des angestrebten Sicherheitsniveaus wird möglich. Bei der Überprüfung des aktuellen Niveaus der Informationssicherheit durch Mitarbeiter der Institution wird neben den technischen Anforderungen meist auch zugleich ersichtlich, in welchen organisatorischen und infrastrukturellen Bereichen Optimierungsbedarf besteht.

Allgemeine Einflussfaktoren

Informationssicherheit auf einem angemessenen Niveau trägt einen elementaren Anteil daran, dass eine Institution ihre Geschäftsziele erreichen kann. Daher müssen die folgenden Einflussfaktoren betrachtet werden:

» **Geschäftsziele:** Welche Faktoren sind wesentlich für den Erfolg des Unternehmens oder der Behörde? Welche Produkte, Angebote und Aufträge bilden die Grundlage der Geschäftstätigkeit? Was sind die generellen Ziele der Institution? Welche Rolle spielt Informationssicherheit hierbei?

» **Organisationsstruktur:** Wie ist die Institution organisiert und strukturiert? Welche Managementsysteme sind vorhanden (beispielsweise Risikomanagement oder Qualitätsmanagement)?

» **Zusammenarbeit mit Externen:** Wer sind die wichtigsten Kunden, Partner und Gremien? Welche grundlegenden Anforderungen und Erwartungen an die Informationssicherheit der Institution bringen sie mit? Wer sind die wichtigsten Dienstleister und Zulieferer? Welche Rolle spielen diese für die Informationssicherheit der Institution?

» **Strategischer Kontext:** Was sind die wesentlichen Herausforderungen für die Institution? Wie ist die Wettbewerbsposition?

Rahmenbedingungen – intern und extern

Viele interne und externe Rahmenbedingungen können Auswirkungen auf die Informationssicherheit haben und müssen folglich ermittelt werden. Über die Analyse der Geschäftsprozesse (einschließlich Fachaufgaben) lassen sich Aussagen über die möglichen Auswirkungen von Sicherheitsvorfällen auf die Geschäftstätigkeit und die Aufgabenerfüllung ableiten. In vielen Institutionen existieren bereits Übersichten zu Geschäftsprozessen, Objekten oder Datensammlungen, die für betriebliche Aspekte oder die Verwaltung benötigt werden. Falls vorhanden, können vorliegende Prozesslandkarten, Geschäftsverteilungspläne, Datenbanken, Übersichten, Netzpläne und Inventarisierungstools genutzt werden, um die wesentlichen Geschäftsprozesse zu identifizieren. Werden diese Übersichten berücksichtigt, sollte darauf geachtet werden, dass die Erfassung nicht zu detailliert gerät. Ziel ist ein erster grober Überblick, welche Informationen für einen Geschäftsprozess mit welchen Anwendungen und IT-Systemen verarbeitet werden. Auf dieser Grundlage können weitere Entscheidungen getroffen werden.

Auf einen Blick: Wichtige interne und externe Rahmenbedingungen abklären

» Welche Geschäftsprozesse gibt es in der Institution und wie hängen diese mit den Geschäftszielen zusammen?

» Welche Geschäftsprozesse hängen von einer funktionierenden Informationstechnik ab?

» Welche Informationen werden bei diesen Geschäftsprozessen verarbeitet?

» Welche Informationen sind besonders wichtig und damit in Bezug auf Vertraulichkeit, Integrität und Verfügbarkeit schützenswert, und warum (z. B. personenbezogene Daten, Kundendaten, sensible Firmeninterna)?

» Zu jedem Geschäftsprozess und zu jeder Fachaufgabe muss ein verantwortlicher Ansprechpartner benannt werden.

» Was sind die gesetzlichen Rahmenbedingungen (nationale und internationale Gesetze und Bestimmungen)?

» Wie sehen Anforderungen von Kunden, Lieferanten und Geschäftspartnern, die aktuelle Marktlage, Wettbewerbssituation und weitere relevante marktspezifische Abhängigkeiten aus?

» Was sind branchenspezifische Sicherheitsstandards?

Brainstorming: Ermittlung der Rahmenbedingungen

Um alle Rahmenbedingungen für die wesentlichen Geschäftsprozesse möglichst schnell und umfassend zu ermitteln, empfiehlt es sich, zu jedem Geschäftsprozess ein kurzes Brainstorming durchzuführen. Diese Gespräche sollten unter der Leitung des ISB mit den jeweiligen Fachverantwortlichen sowie dem entsprechenden IT-Verantwortlichen durchgeführt werden.

Im Fokus der internen Erhebung sollten vorrangig geschäftskritische Informationen und Kernprozesse stehen sowie die zugehörigen Anwendungen, IT-Systeme, Netze und Räume. Ausgehend von den Kernprozessen sollten zudem die wesentlichen unterstützenden Prozesse und die hauptsächlich betroffenen Objekte ermittelt werden.

Ersterfassung der Prozesse, Anwendungen und IT-Systeme

Die Ergebnisse der vorherigen Schritte, das heißt die Ermittlung von Rahmenbedingungen und die Formulierung von Informationssicherheitszielen, sollten als nächstes in einer Übersicht mit den vorhandenen Werten der Institution konsolidiert werden.

Da ein Informationsverbund meist aus vielen Einzelobjekten besteht, ist es häufig nicht zweckmäßig, jedes Objekt einzeln zu erfassen. Stattdessen hat es sich in der Praxis als hilfreich erwiesen, ähnliche Objekte zu Gruppen zusammenzufassen. Möglich ist auch, zunächst eine grafische Netzübersicht zu erstellen und ausgehend von dieser die IT-Systeme zu erfassen. Die Darstellung der Netzübersicht kann dabei stark vereinfacht sein. Auch IT-Systeme oder Prozesse, die etwa im Rahmen eines Outsourcings ausgelagert wurden oder in der Cloud betrieben werden, sollten hier aufgeführt werden.

Bei der Ersterfassung sollten nur die wesentlichen Objekte erfasst werden. Beispielsweise sollten Serverräume mit einem meist höheren Sicherheitsniveau aufgenommen werden, die klassischen Büroräume eher nicht. Als Ergebnis der Ersterfassung sollte eine Übersicht vorliegen, die mit überschaubaren Ressourcen herstellbar ist.

Auf einen Blick: Erfassung der relevanten Objekte

» Geschäftsprozess oder Fachaufgabe:
Name und (falls erforderlich) Beschreibung, Fachverantwortlicher

» Anwendung:
Name, (falls erforderlich) Beschreibung und dazugehöriger Geschäftsprozess

» IT-, ICS-Systeme und sonstige Objekte:
Name, Plattform und sofern sinnvoll Aufstellungsort

» Betriebsrelevante Räume, die ein höheres Sicherheitsniveau erfordern (z.B. Serverräume):
Art, Raumnummer und Gebäude

Abschätzung des Sicherheitsniveaus

Für spätere Betrachtungen kann es sich als sinnvoll erweisen, schon zu einem frühen Zeitpunkt das angestrebte Sicherheitsniveau der einzelnen Assets, also der Zielobjekte, abzuschätzen. Diese erste Abschätzung des Sicherheitsniveaus bietet eine grobe Orientierung für den zu erwartenden Aufwand und erleichtert eine geeignete Gruppenbildung der identifizierten Assets.

Die bisher identifizierten Objekte, bei denen ein höheres Sicherheitsniveau als „normal“ angestrebt wird, sollten in der bereits erstellten Tabelle gekennzeichnet werden.

Erstellung eines grafischen Netzplans

Auf Grundlage der erfassten Informationen sollte zur besseren Übersicht ein rudimentärer Netzplan erstellt werden. Diese Netzübersicht dient als Überblick, der die weitere Diskussion vereinfachen und zeigen kann, ob essentielle IT-Systeme übersehen wurden. Der Plan sollte mindestens die folgenden Objekte beinhalten:

» IT-Systeme, d. h. Clients und Server sowie aktive Netzkomponenten,

» Netzverbindungen zwischen diesen Systemen,

» Verbindungen des betrachteten Bereichs nach außen.

Die grafische Netzübersicht sollte nicht nur physische Komponenten enthalten, sondern auch virtualisierte Strukturen. Hierbei können entweder virtuelle Strukturen direkt in die Netzübersicht aufgenommen oder bei unübersichtlicheren Architekturen in eine separate Netzübersicht eingetragen werden. Dies gilt ebenfalls für solche IT-Systeme und Prozesse, die ausgelagert sind. Ein Beispiel für eine Ersterfassung einschließlich einer Netzübersicht ist in den Hilfsmitteln zum IT-Grundschutz auf den Webseiten des BSI zu finden. In der später durchzuführenden Strukturanalyse werden die hier gewonnenen Ergebnisse präzisiert und vervollständigt.

Auf einen Blick: Konzeption und Planung des Sicherheitsprozesses

» Ansprechpartner für alle Geschäftsprozesse und Fachaufgaben benennen

» Grobeinschätzung der Wertigkeit und des Sicherheitsniveaus von Informationen, Geschäftsprozessen und Fachaufgaben durchführen

» Interne und externe Rahmenbedingungen ermitteln

» Bedeutung der Geschäftsprozesse, Fachaufgaben und Informationen abschätzen

» Allgemeine Informationssicherheitsziele festlegen

» Konsolidierte Übersicht der vorhandenen Assets mit den zuvor gewonnenen Erkenntnissen erstellen

Dokumentation im Sicherheitsprozess

Entscheidungen sollten stets nachvollziehbar und wiederholbar sein. Vor und während des Sicherheitsprozesses wird daher eine Vielzahl unterschiedlicher Dokumente erstellt. Hierbei sollte immer darauf geachtet werden, dass der Aufwand für die Erstellung von Dokumentationen in einem angemessenen Rahmen bleibt. Wenn bei der Umsetzung der IT-Grundschutz-Methodik etwas dokumentiert werden muss, ist es dafür meistens nicht erforderlich, neue Dokumente zu erstellen. Im Allgemeinen reicht es, die notwendigen Informationen an geeigneter Stelle zu sammeln bzw. zu notieren.

Besonders bei der Basis-Absicherung sollte der Dokumentationsprozess möglichst einfach und zweckmäßig gehalten werden.

3.3 Durchführung des Sicherheitsprozesses

Nachdem der Sicherheitsprozess initiiert worden ist und alle organisatorischen Aufgaben abgearbeitet wurden, beginnt mit der eigentlichen Durchführung bereits die wichtige letzte Phase im Rahmen der Basis-Absicherung: die Erstellung und Umsetzung der Sicherheitskonzeption.

Für die Sicherheitskonzeption sollten für typische Komponenten von Geschäftsprozessen, Anwendungen und IT-Systemen organisatorische, personelle, infrastrukturelle und technische Anforderungen aus dem IT-Grundschutz-Kompendium erfüllt werden. Diese sind nach unterschiedlichen Themen strukturiert in den Bausteinen beschrieben, mit denen modular gearbeitet werden kann. Im Rahmen einer Basis-Absicherung müssen lediglich die Basisanforderungen betrachtet werden.

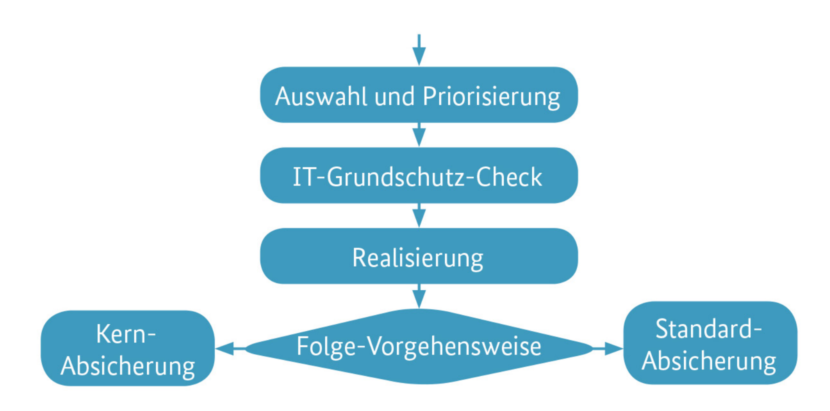


Abbildung 3: Schematisches Vorgehen nach der Basis-Absicherung

Nachdem im vorherigen Schritt zur Organisation des Sicherheitsprozesses der Geltungsbereich festgelegt wurde, gliedert sich die Erstellung einer Sicherheitskonzeption nach der Basis-Absicherung nun in folgende Aktionsfelder, die anschließend detailliert vorgestellt werden:

» **Auswahl und Priorisierung:**
Der betrachtete Informationsverbund muss mit Hilfe der vorhandenen Bausteine aus dem IT-Grundschutz-Kompendium nachgebildet werden.

» **IT-Grundschutz-Check:**
In diesem Schritt wird überprüft, ob oder inwieweit die in den Basisanforderungen nach IT-Grundschutz formulierten Vorgaben bereits erfüllt sind und welche Sicherheitsmaßnahmen noch fehlen.

» **Realisierung:**
Für die bisher nicht erfüllten Basisanforderungen müssen geeignete Sicherheitsmaßnahmen festgelegt und umgesetzt werden.

» **Auswahl der folgenden Vorgehensweise:**
Die Basis-Absicherung dient als Einstiegsvorgehensweise. Es muss daher festgelegt werden, zu welchem Zeitpunkt und mit welcher IT-Grundschutz-Vorgehensweise das Sicherheitsniveau weiter angehoben werden soll.

3.3.1 Auswahl und Priorisierung der Bausteine (Modellierung)

Zunächst wird der betrachtete Informationsverbund auf Basis der in der Ersterfassung identifizierten Prozesse, Anwendungen, IT-Systeme, Kommunikationsverbindungen und Räume sowie den vorhandenen Bausteinen aus dem IT-Grundschutz-Kompendium nachgebildet. Das Ergebnis ist ein IT-Grundschutz-Modell des Informationsverbunds, das aus unterschiedlichen, gegebenenfalls mehrfach verwendeten Bausteinen besteht und dadurch die sicherheitsrelevanten Aspekte des Informationsverbunds beinhaltet.

Modellierung nach IT-Grundschutz

Um einen meist komplexen Informationsverbund nach IT-Grundschutz zu modellieren, müssen die passenden Bausteine aus dem IT-Grundschutz-Kompendium ausgewählt und umgesetzt werden. Zur besseren Handhabbarkeit sind die Bausteine im IT-Grundschutz-Kompendium in prozess- und systemorientierte Bausteine sowie verschiedene Schichten aufgeteilt. Nähere Details zum Aufbau und zu den Inhalten finden sich im Anhang „Das IT-Grundschutz-Kompendium – Wissenswertes auf einen Blick“.

Die Modellierung nach IT-Grundschutz besteht nun darin, Bausteine oder einzelne Aspekte zur Abbildung des Informationsverbunds auszuwählen. Je nach Baustein können die

Zielobjekte unterschiedlich sein: einzelne Geschäftsprozesse oder Komponenten, Gruppen von Komponenten, Gebäude, Liegenschaften, Organisationseinheiten usw. Können einzelne Zielobjekte nicht mit den Bausteinen abgebildet werden, müssen stattdessen vergleichbare oder übergeordnete Bausteine herangezogen werden.

Reihenfolge der Baustein-Umsetzung

Um grundlegende Risiken zu minimieren und Informationssicherheit ganzheitlich aufzubauen, müssen die essentiellen Sicherheitsanforderungen frühzeitig erfüllt und entsprechende Sicherheitsmaßnahmen umgesetzt werden. Die IT-Grundschutz-Methodik rät daher zu einer bestimmten Reihenfolge bei der Umsetzung der Bausteine. Im IT-Grundschutz-Kompendium wird im Kapitel „Schichtenmodell und Modellierung" beschrieben, wann ein einzelner Baustein sinnvollerweise eingesetzt werden soll und auf welche Zielobjekte er anzuwenden ist. Die Bausteine sind entsprechend gekennzeichnet, ob sie vor- oder nachrangig umgesetzt werden sollten.

Diese Kennzeichnung zeigt eine sinnvolle zeitliche Reihenfolge für die Umsetzung der jeweiligen Anforderungen auf, sie gewichtet die Bausteine jedoch nicht untereinander. Grundsätzlich müssen alle relevanten Bausteine aus dem IT-Grundschutz-Kompendium für einen Informationsverbund umgesetzt werden. Jede Institution kann eine abweichende, für sich sinnvolle Reihenfolge festlegen.

Das erstellte IT-Grundschutz-Modell ist unabhängig davon, ob der Informationsverbund aus bereits im Einsatz befindlichen Komponenten besteht oder ob es sich um einen Informationsverbund handelt, der geplant wird. Das Modell kann daher unterschiedlich verwendet werden:

» Der ISB kann mit dem IT-Grundschutz-Modell eines bestehenden Informationsverbundes auf Basis der Bausteine relevante Sicherheitsanforderungen identifizieren. Es kann in Form eines **Prüfplans** benutzt werden, um einen Soll-Ist-Vergleich durchzuführen.

» Das IT-Grundschutz-Modell eines geplanten Informationsverbundes stellt hingegen einen **Entwicklungsplan** dar. Es beschreibt mit den ausgewählten Bausteinen, welche Sicherheitsanforderungen bei der Realisierung des Informationsverbunds erfüllt werden müssen.

Die Einordnung der Modellierung und die möglichen Ergebnisse verdeutlicht die folgende schematische Darstellung:

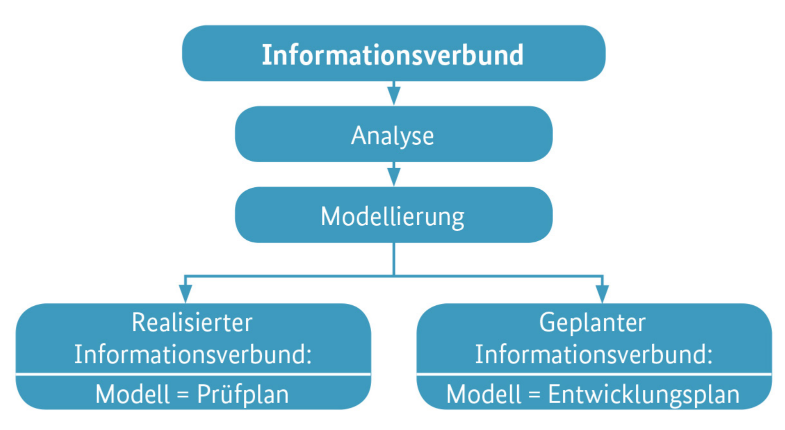


Abbildung 4: Ergebnis der Modellierung nach IT-Grundschutz

In der Regel enthält ein Informationsverbund sowohl bereits existierende als auch geplante Anteile, so dass das resultierende IT-Grundschutz-Modell sowohl einen Prüfplan als auch Anteile eines Entwicklungsplans enthält. Alle Sicherheitsanforderungen bilden damit gemeinsam die Basis für die Erstellung des Sicherheitskonzepts:

» bereits erfüllte Sicherheitsanforderungen,

» die bei Durchführung des Soll-Ist-Vergleichs als unzureichend oder gar nicht erfüllt identifizierten Anforderungen sowie

» Anforderungen, die sich für die in Planung befindlichen Anteile des Informationsverbunds ergeben.

Zuordnung von Bausteinen

Die Zuordnung von Bausteinen zu Zielobjekten sollte in Form einer Tabelle mit folgenden Spalten dokumentiert werden:

» Vollständiger Titel und Nummer des Bausteins (z. B. SYS.3.1 Laptop)

» Zielobjekt oder Zielgruppe: Dies kann z. B. die Identifikationsnummer einer Komponente oder einer Gruppe bzw. der Name eines Gebäudes oder einer Organisationseinheit sein.

» Ansprechpartner: Diese Spalte dient zunächst nur als Platzhalter. Der Ansprechpartner wird nicht im Rahmen der Modellierung, sondern erst bei der Planung des eigentlichen Soll-Ist-Vergleichs im IT-Grundschutz-Check ermittelt.

» Reihenfolge: Es sollte die Umsetzungsreihenfolge (R1, R2, R3) des Bausteins eingetragen werden.

» Hinweise: In dieser Spalte können ergänzende Informationen oder Begründungen für die Modellierung dokumentiert werden.

Auf einen Blick: Modellierung eines Informationsverbunds

- » Kapitel „Schichtenmodell und Modellierung“ aus dem IT-Grundschutz-Kompendium systematisch durcharbeiten.
- » Für jeden Baustein des IT-Grundschutz-Kompendiums ermitteln, auf welche Zielobjekte er im betrachteten Informationsverbund anzuwenden ist.
- » Zuordnung von Bausteinen zu Zielobjekten („IT-Grundschutz-Modell“) sowie die entsprechenden Ansprechpartner dokumentieren.
- » Zielobjekte, die nicht geeignet modelliert werden können, vormerken.
- » Reihenfolge für die Umsetzung der Bausteine festlegen.

3.3.2 IT-Grundschutz-Check für Basis-Absicherung

Die Auswahl und Priorisierung der IT-Grundschutz-Bausteine wird beim weiteren Vorgehen als Prüfplan bezeichnet. Anhand eines Soll-Ist-Vergleichs gilt es herauszufinden, welche Basisanforderungen ausreichend oder nur unzureichend bzw. gar nicht erfüllt sind.

Bei einem IT-Grundschutz-Check für die Basis-Absicherung müssen lediglich die Basisanforderungen erfüllt sein. Für eine möglicherweise spätere Standard- oder Kern-Absicherung ist dann ein separater IT-Grundschutz-Check durchzuführen, bei dem die Standard-Anforderungen der betreffenden Bausteine hinzukommen. Um Mehraufwand zu vermeiden und Synergieeffekte nutzen zu können, sollten die Ergebnisse des IT-Grund-

schutz-Checks für die Basis-Absicherung so aufbereitet sein, dass sie zu einem späteren Zeitpunkt direkt in die Standard- oder Kern-Absicherung integriert werden können.

Der IT-Grundschutz-Check besteht aus drei unterschiedlichen Schritten: Im ersten Schritt werden die organisatorischen Vorbereitungen getroffen und relevante Ansprechpartner für den Soll-Ist-Vergleich ausgewählt. Im zweiten Schritt wird der eigentliche Soll-Ist-Vergleich mittels Interviews und Stichproben durchgeführt. Im letzten Schritt werden die erzielten Ergebnisse des Soll-Ist-Vergleichs einschließlich der erhobenen Begründungen dokumentiert.

Schritt 1: Organisatorische Vorbereitungen

Für die reibungslose Durchführung des Soll-Ist-Vergleichs sind einige Vorarbeiten erforderlich. Zunächst sollten alle hausinternen Papiere, z. B. Organisationsverfügungen, Arbeitshinweise, Sicherheitsanweisungen, Handbücher und „informelle" Vorgehensweisen, die die sicherheitsrelevanten Abläufe regeln, gesichtet werden. Diese Dokumente können bei der Ermittlung des Umsetzungsgrades hilfreich sein, insbesondere bei Fragen nach bestehenden organisatorischen Regelungen. Weiterhin ist zu klären, wer gegenwärtig für deren Inhalt zuständig ist, um später die richtigen Ansprechpartner bestimmen zu können.

Als Nächstes sollte festgestellt werden, ob und in welchem Umfang externe Stellen bei der Ermittlung des Umsetzungsstatus beteiligt werden müssen. Dies kann beispielsweise bei ausgelagerten Rechenzentren, vorgesetzten Behörden oder Firmen, die Teile von Geschäftsprozessen oder des IT-Betriebes als Outsourcing-Dienstleistung übernehmen, erforderlich sein.

Ein wichtiger Aspekt ist, geeignete Ansprechpartner für die einzelnen Bausteine zu ermitteln, die für die Modellierung des vorliegenden Informationsverbunds herangezogen wurden. Bei den Anforderungen in den Bausteinen werden die Rollen genannt, die für die jeweilige Umsetzung zuständig sind. Hieraus können die Ansprechpartner für die jeweilige Thematik in der Institution identifiziert werden. Im Folgenden finden sich einige Beispiele für Ansprechpartner der verschiedenen Bereiche:

» Bei den Bausteinen der Schicht ORP, CON und OPS ergibt sich ein geeigneter Ansprechpartner in der Regel direkt aus der im Baustein behandelten Thematik. Beispielsweise sollte für den Baustein ORP.2 „Personal" ein Mitarbeiter der zuständigen Personalabteilung als Ansprechpartner ausgewählt werden. Bei den konzeptionellen Bausteinen sollte derjenige Mitarbeiter befragt werden, zu dessen Aufgabengebiet die Fortschreibung von Regelungen in dem betrachteten Bereich gehören.

» Im Bereich der Schicht INF „Infrastruktur" sollte die Auswahl geeigneter Ansprechpartner in Abstimmung mit der Haustechnik vorgenommen werden. Je nach Größe der betrachteten Institution können beispielsweise unterschiedliche Ansprechpartner für die Infrastrukturbereiche Gebäude und Technikräume zuständig sein. In kleinen Institutionen kann in vielen Fällen der Hausmeister Auskunft geben.

» In den systemorientierten Bausteinen der Schichten SYS, NET und IND werden in den zu prüfenden Sicherheitsmaßnahmen verstärkt technische Aspekte behandelt. In der Regel kommt daher die Administratoren dieser Komponenten bzw. Gruppen von Komponenten als Ansprechpartner in Frage.

» Für die Bausteine der Schicht APP „Anwendungen“ sollten die Verantwortlichen für die einzelnen Anwendungen als Hauptansprechpartner ausgewählt werden.

Übersicht: Organisatorische Vorarbeiten des IT-Grundschutz-Checks

» Hausinterne Dokumente mit Verfügungen und Regelungen sichten und Zuständigkeiten für diese Unterlagen klären.

» Feststellen, in welchem Umfang externe Stellen beteiligt werden müssen.

» Hauptansprechpartner für jeden in der Modellierung angewandten Baustein festlegen.

Schritt 2: Durchführung des Soll-Ist-Vergleichs

Sind alle erforderlichen Vorarbeiten erledigt, werden die Sicherheitsanforderungen des jeweiligen Bausteins, für den die Ansprechpartner zuständig sind, gemeinsam mit diesen der Reihe nach durchgearbeitet. Den Befragten sollte zudem der Zweck des IT-Grundschutz-Checks kurz vorgestellt werden. Falls Bedarf besteht, die gemachten Aussagen zu verifizieren, bietet es sich an, stichprobenartig die entsprechenden Regelungen und Konzepte zu sichten. Im Bereich Infrastruktur könnten beispielsweise die zu untersuchenden Objekte gemeinsam mit dem Ansprechpartner vor Ort besichtigt werden. Außerdem könnten z. B. Client- bzw. Servereinstellungen an ausgewählten IT-Systemen gemeinsam überprüft werden.

Am Ende sollte zwischen dem ISB und dem jeweiligen Ansprechpartner Einvernehmen über den Umsetzungsstatus bestehen.

Als Antworten bezüglich des Umsetzungsstatus der einzelnen Anforderungen kommen folgende Aussagen in Betracht:

„entbehrlich“	Die Erfüllung der Anforderung ist in der vorgeschlagenen Art nicht notwendig, weil die Anforderung im betrachteten Informationsverbund nicht relevant ist (z. B. weil Dienste nicht aktiviert wurden) oder bereits durch Alternativmaßnahmen erfüllt wurde. Wird der Umsetzungsstatus einer Anforderung auf „entbehrlich“ gesetzt, müssen über die Kreuzreferenztabelle des jeweiligen Bausteins die zugehörigen elementaren Gefährdungen identifiziert werden. Wurden Alternativmaßnahmen ergriffen, muss begründet werden, dass das Risiko, das von allen betreffenden elementaren Gefährdungen ausgeht, angemessen minimiert wurde. Wenn Basisanforderungen nicht erfüllt werden, bleibt grundsätzlich ein erhöhtes Risiko bestehen. Anforderungen dürfen nicht auf „entbehrlich“ gesetzt werden, indem das Risiko für eine im Baustein identifizierte elementare Gefährdung über die Kreuzreferenztabelle pauschal akzeptiert oder ausgeschlossen wird.
„ja“	Zu der Anforderung wurden geeignete Maßnahmen vollständig, wirksam und angemessen umgesetzt.
„teilweise“	Die Anforderung wurde nur teilweise umgesetzt.

„nein“	Die Anforderung wurde noch nicht erfüllt, also geeignete Maßnahmen sind größtenteils noch nicht umgesetzt worden.

Es ist sinnvoll, bei den Interviews nicht nur die Bausteintexte, sondern auch die Umsetzungshinweise oder andere ergänzende Materialien griffbereit zu haben.

Übersicht: Durchführung des Soll-Ist-Vergleichs

» Je nach Fachgebiet vorab Checklisten erstellen.

» Umsetzungsstatus der einzelnen Anforderungen mit dem Ansprechpartner erarbeiten.

» Falls erforderlich, Umsetzungsstatus anhand von Stichproben am Objekt verifizieren.

Schritt 3: Dokumentationen der Ergebnisse

Die Ergebnisse des IT-Grundschutz-Checks sollten so dokumentiert werden, dass sie für alle Beteiligten nachvollziehbar sind und als Grundlage für die Umsetzungsplanung der identifizierten Maßnahmen genutzt werden können.

Zur Dokumentation des IT-Grundschutz-Checks sollten erfasst werden:

» Die Nummer und die Bezeichnung des Objektes oder der Gruppe von Objekten, welcher der Baustein bei der Modellierung zugeordnet wurde,

» der Standort der zugeordneten Objekte bzw. Gruppe von Objekten,

» das Erfassungsdatum und der Name des Erfassers und

» die befragten Ansprechpartner.

Die Ergebnisse des Soll-Ist-Vergleichs sollten tabellarisch erfasst werden. Dabei sollten zu jeder Anforderung des jeweiligen Bausteins folgende Informationen festgehalten werden:

» **Umsetzungsgrad** (entbehrlich/ja/teilweise/nein)
Der im Interview ermittelte Umsetzungsstatus der jeweiligen Anforderung ist zu erfassen.

» **Termin für die Umsetzung**
Ein solches Feld ist sinnvoll, auch wenn es während eines IT-Grundschutz-Checks im Allgemeinen nicht ausgefüllt wird. Es dient als Platzhalter, um in der Realisierungsplanung an dieser Stelle zu dokumentieren, bis zu welchem Termin die Anforderung vollständig umgesetzt sein soll.

» **Verantwortliche**
Falls es bei der Durchführung des Soll-Ist-Vergleichs eindeutig ist, welche Mitarbeiter für die vollständige Umsetzung einer noch nicht erfüllten Anforderung oder Maßnahme verantwortlich sind, sollte das namentlich in diesem Feld dokumentiert werden. Andernfalls ist im Zuge der späteren Realisierungsplanung ein Verantwortlicher zu bestimmen.

» **Bemerkungen/Begründungen**
Ein solches Feld ist wichtig, um getroffene Entscheidungen später nachvollziehen zu können. Bei Anforderungen, deren Umsetzung entbehrlich erscheint, ist hier die Begründung zu nennen. Bei Anforderungen, die noch nicht oder nur teilweise

umgesetzt sind, sollte in diesem Feld dokumentiert werden, welche Maßnahmen noch umgesetzt werden müssen. In dieses Feld sollten auch alle anderen Bemerkungen eingetragen werden, die bei der Beseitigung von Defiziten hilfreich oder im Zusammenhang mit der Anforderung zu berücksichtigen sind.

» **Defizite/Kostenschätzung**
Für Anforderungen, die nicht oder nur teilweise erfüllt wurden, ist das damit verbundene Risiko in geeigneter Form zu ermitteln und zu dokumentieren. Bei solchen Maßnahmen sollte außerdem geschätzt werden, welchen finanziellen und personellen Aufwand die Beseitigung der Defizite erfordert.

Auf den Webseiten des BSI stehen für alle Bausteine des IT-Grundschutz-Kompendiums Formulare zur Verfügung, die als Hilfsmittel für die Dokumentation des IT-Grundschutz-Checks verwendet werden können.

Übersicht: Dokumentation der Ergebnisse

» Stamminformationen über jedes Zielobjekt erfassen

» Informationen zum IT-Grundschutz-Check und zum Umsetzungsstatus dokumentieren

» Felder beziehungsweise Platzhalter für die Realisierungsplanung vorsehen

3.3.3 Umsetzung der Sicherheitskonzeption

Zu diesem Zeitpunkt liegen die Ergebnisse des IT-Grundschutz-Checks, also ein Soll-Ist-Vergleich, vor. In diesem Kapitel wird

beschrieben, wie die Umsetzung der notwendigen Sicherheitsmaßnahmen geplant, durchgeführt, begleitet und überwacht werden kann. Zu vielen Bausteinen des IT-Grundschutzes existieren Umsetzungshinweise mit beispielhaften Empfehlungen für Sicherheitsmaßnahmen, mit denen die Anforderungen der Bausteine umgesetzt werden können. Diese basieren auf Best Practices und langjähriger Erfahrung von Experten aus dem Bereich der Informationssicherheit. Die Maßnahmen aus den Umsetzungshinweisen sind jedoch nicht als verbindlich zu betrachten, sie können auch durch eigene Maßnahmen ergänzt oder ersetzt werden.

Für die Realisierung der Maßnahmen stehen in der Regel nur begrenzte finanzielle und personelle Ressourcen zur Verfügung. Ziel der nachfolgend beschriebenen Schritte ist daher, die geplanten Sicherheitsmaßnahmen möglichst effizient umzusetzen.

Festlegung konkreter Maßnahmen zu den Anforderungen

In einer Gesamtsicht sollte auf Basis des IT-Grundschutz-Checks ausgewertet werden, welche Anforderungen aus den IT-Grundschutz-Bausteinen nicht oder nur teilweise umgesetzt wurden.

Bei der Modellierung wurden diejenigen Bausteine ausgewählt, die für die einzelnen Zielobjekte des betrachteten Informationsverbunds umzusetzen sind. In den Bausteinen sind die Anforderungen beschrieben, die typischerweise für diese Komponenten für ein angemessenes Sicherheitsniveau umgesetzt werden müssen. Im Rahmen einer Basis-Absicherung müssen lediglich die Basisanforderungen betrachtet werden. Diese sind so elementar, dass sie für eine grundlegende Absicherung des Informationsverbundes umgesetzt werden müssen. Zudem

bringt die Erfüllung der Basisanforderungen in der Regel gute Ergebnisse bei vergleichsweise niedrigem Einsatz von Ressourcen, sogenannte Quick Wins. Die Standardanforderungen sowie die Anforderungen bei erhöhtem Schutzbedarf sind für die Vorgehensweisen der Standard- und Kern-Absicherung relevant. Aber auch im Rahmen der Basis-Absicherung kann es sich lohnen, einen Blick auf diese Anforderungen zu werfen, um das Sicherheitsniveau weiter zu erhöhen.

Die Anforderungen in den Bausteinen sind knapp und präzise formuliert. Sie müssen passend zu den organisatorischen und technischen Gegebenheiten der Institution in konkrete Sicherheitsmaßnahmen umgesetzt werden, welche die jeweiligen Anforderungen erfüllen.

Die Maßnahmen dienen als Handlungsvorgaben für die verschiedenen Akteure im Sicherheitsprozess. Sie müssen daher

» an die jeweiligen Rahmenbedingungen und den Sprachgebrauch einer Institution angepasst sein und

» ausreichend konkret sein, um im betrachteten Informationsverbund angewendet werden zu können, also z. B. technische Details enthalten.

Generell sollten die Anforderungen der IT-Grundschutz-Bausteine immer sinngemäß umgesetzt werden. Alle Änderungen zum IT-Grundschutz-Kompendium sollten zur besseren Nachvollziehbarkeit dokumentiert werden.

Zu vielen Bausteinen des IT-Grundschutz-Kompendiums gibt es Umsetzungshinweise, in denen zu den Sicherheitsanforderungen bereits detailliertere und praxiserprobte Maßnahmen beschrieben sind. Diese Maßnahmen sind einerseits so allgemein formuliert, dass sie in möglichst vielen Umgebungen

anwendbar sind, und andererseits so ausführlich, dass die Maßnahmenbeschreibungen als Umsetzungshilfe dienen können.

Auch die in den Umsetzungshinweisen vorgeschlagenen Maßnahmen sollten noch an die jeweiligen Rahmenbedingungen einer Institution angepasst werden. Es kann beispielsweise sinnvoll sein,

» Maßnahmen weiter zu konkretisieren, also z. B. um technische Details zu ergänzen,

» Maßnahmen dem Sprachgebrauch der Institution anzupassen, also z. B. andere Rollenbezeichnungen zu verwenden und

» aus Maßnahmen, die im betrachteten Bereich nicht relevanten Empfehlungen zu streichen.

Wichtig ist außerdem, realisierungsbegleitende Maßnahmen mit einzuplanen. Hierzu gehören z. B. Maßnahmen zur Sensibilisierung der Mitarbeiter, um die Belange der Informationssicherheit sowie die Notwendigkeit und die Konsequenzen der Maßnahmen zu verdeutlichen.

In seltenen Fällen kann es sich auch bei den elementaren Basisanforderungen ergeben, dass einzelne Anforderungen unter den konkreten Rahmenbedingungen nicht umgesetzt werden können, etwa wenn deren Umsetzung essentielle Schwierigkeiten in anderen Bereichen mit sich bringen würde. Dies kann beispielsweise der Fall sein, wenn sich Anforderungen des Brand- und des Einbruchschutzes nicht miteinander vereinbaren lassen. Dann müssen andere Lösungen gefunden und dies nachvollziehbar dokumentiert werden.

Um auch später noch nachvollziehen zu können, wie die konkrete Maßnahmenliste erstellt und angepasst wurde, sollte

sie dokumentiert werden. Werden Sicherheitsanforderungen zusätzlich aufgenommen oder geändert, ist auch dies im Sicherheitskonzept zu dokumentieren. Bei der Auswahl und Anpassung der Sicherheitsmaßnahmen auf Basis der Anforderungen ist zu beachten, dass diese immer angemessen sein müssen. Angemessen bedeutet:

» **Wirksamkeit (Effektivität):** Die Maßnahmen müssen vor den möglichen Gefährdungen wirksam schützen, also den identifizierten Schutzbedarf abdecken.

» **Eignung:** Sie müssen in der Praxis umsetzbar sein, dürfen also z. B. die Organisationsabläufe nicht zu stark behindern oder andere Sicherheitsmaßnahmen aushebeln.

» **Praktikabilität:** Sie sollen leicht verständlich, einfach anzuwenden und wenig fehleranfällig sein.

» **Akzeptanz:** Sie müssen für alle Benutzer einfach anwendbar sein und dürfen niemanden diskriminieren oder beeinträchtigen.

» **Wirtschaftlichkeit:** Mit den eingesetzten Mitteln sollte ein möglichst gutes Ergebnis erreicht werden. Die Sicherheitsmaßnahmen sollten also einerseits das Risiko bestmöglich minimieren und andererseits in geeignetem Verhältnis zu den zu schützenden Werten stehen.

Kosten- und Aufwandsschätzung

Da das Budget zur Umsetzung von Sicherheitsmaßnahmen praktisch immer begrenzt ist, sollte für jede zu realisierende Maßnahme festgehalten werden, welche Investitionskosten und welcher Personalaufwand dafür benötigt werden. Hierbei

sollte zwischen einmaligen und wiederkehrenden Investitionskosten bzw. Personalaufwand unterschieden werden. An dieser Stelle zeigt sich häufig, dass Einsparungen bei technischen oder infrastrukturellen Sicherheitsmaßnahmen dazu führen, dass sie einen hohen fortlaufenden Personaleinsatz verursachen. Umgekehrt führen Einsparungen beim Personal schnell zu kontinuierlich größer werdenden Sicherheitsdefiziten.

In diesem Zusammenhang ist zu ermitteln, ob alle identifizierten Maßnahmen wirtschaftlich umsetzbar sind. Falls es Maßnahmen gibt, die nicht wirtschaftlich sind, sollte überlegt werden, durch welche Ersatzmaßnahmen die Anforderungen dennoch erfüllt werden können. Oftmals gibt es verschiedene Optionen, Anforderungen mit geeigneten Maßnahmen zu erfüllen. Dabei ist zu beachten, dass Basisanforderungen im Normalfall immer erfüllt werden müssen, die Akzeptanz eines Restrisikos ist aufgrund ihrer elementaren Natur nicht vorgesehen.

Liegen Einschätzungen für Kosten und Personaleinsatz vor, muss meist noch im Detail entschieden werden, wie viel Ressourcen für die Umsetzung der Sicherheitsmaßnahmen eingesetzt werden sollen. Die Ergebnisse der Sicherheitsuntersuchung sollten daher der Institutionsleitung vorgestellt werden. Dazu zählen die festgestellten Schwachstellen (also nicht oder unzureichend erfüllte Sicherheitsanforderungen) sowie die zu erwartenden Kosten und Aufwände für Umsetzung der notwendigen Maßnahmen. Die Leitung kann auf dieser Basis über das freizugebende Budget entscheiden.

Sofern kein ausreichendes Budget für die Realisierung aller fehlenden Maßnahmen bereitgestellt werden kann, sollte das verbleibende Restrisiko aufgezeigt werden. Dazu können die sogenannten Kreuzreferenztabellen aus den einzelnen Bausteinen hinzugezogen werden. Die Kreuzreferenztabellen

geben eine Übersicht darüber, welche Anforderungen gegen welche elementaren Gefährdungen wirken. Umgekehrt lässt sich anhand dieser Tabellen ebenfalls ermitteln, gegen welche elementaren Gefährdungen kein ausreichender Schutz besteht, wenn Anforderungen aus den Bausteinen nicht erfüllt werden. Das entstehende Restrisiko sollte transparent beschrieben und der Leitungsebene zur Entscheidung vorgelegt werden. Die Leitungsebene muss die Verantwortung für die Konsequenzen tragen.

Festlegung der Umsetzungsreihenfolge der Maßnahmen

Das IT-Grundschutz-Kompendium beschreibt eine Reihenfolge, in der Bausteine umgesetzt werden sollten, von grundlegenden und übergreifenden Bausteinen bis hin zu solchen, die speziellere Themen abdecken und daher in der zeitlichen Reihenfolge eher nachrangig betrachtet werden können. Diese Reihenfolge der Baustein-Umsetzung ist vor allem bei der Basis-Absicherung wichtig. Für jeden Baustein sind alle aus den Basisanforderungen abgeleiteten Maßnahmen umzusetzen. Ein Blick in die jeweiligen Standard-Anforderungen sowie die Anforderungen für den erhöhten Schutzbedarf kann jedoch ebenfalls sinnvoll sein, da diese häufig ergänzenden Aspekte beschreiben und abdecken.

Wenn das vorhandene Budget oder die personellen Ressourcen nicht ausreichen, um sämtliche noch notwendigen Maßnahmen sofort umsetzen zu können, muss hier eine Priorisierung festgelegt werden.

Die weitere Umsetzungsreihenfolge orientiert sich daran, was für die jeweilige Institution am sinnvollsten ist. Hierzu einige Tipps:

» Bei einigen Maßnahmen ergibt sich durch Abhängigkeiten und logische Zusammenhänge eine zwingende zeitliche Reihenfolge.

» Die Umsetzungsreihenfolge kann darauf basieren, wann die jeweiligen Maßnahmen im Lebenszyklus eines Zielobjektes umzusetzen sind. Bei neuen Zielobjekten sind beispielsweise Maßnahmen aus den Bereichen Planung und Konzeption vor solchen umzusetzen, bei denen es um den sicheren Betrieb geht. Bei schon länger im Informationsverbund vorhandenen Zielobjekten sollte zunächst die Absicherung des Betriebs im Vordergrund stehen.

» Manche Maßnahmen erzielen eine große Breitenwirkung, manche eine stärkere lokale Wirkung. Oft ist es sinnvoll, zuerst auf die Breitenwirkung zu achten. Es lohnt sich aber auch durchaus, die Maßnahmen aus den verschiedenen Bereichen danach zu gewichten, wie schnell sie sich umsetzen lassen und welchen Sicherheitsgewinn sie liefern. Quick Wins lassen sich häufig im organisatorischen Bereich finden oder durch zentrale Konfigurationseinstellungen erreichen.

» Es gibt Bausteine, deren Umsetzung auf das angestrebte Sicherheitsniveau einen größeren Einfluss hat als andere. So sollten beispielsweise immer zunächst die Server abgesichert werden und dann erst die angeschlossenen Clients.

» Bausteine, bei denen im Rahmen des Soll-Ist-Vergleichs auffallend viele Anforderungen als nicht erfüllt identifiziert wurden, repräsentieren Bereiche mit vielen Schwachstellen. Sie sollten ebenfalls bevorzugt behandelt werden.

Festlegung der Aufgaben und der Verantwortung

Nachdem die Reihenfolge für die Umsetzung der Maßnahmen bestimmt wurde, muss festgelegt werden, wer bis wann welche Maßnahmen realisieren muss. Den Verantwortlichen müssen dazu die nötigen Fähigkeiten, Kompetenzen und Ressourcen zur Verfügung stehen.

Ebenso ist festzulegen, wer für die Überwachung der Realisierung verantwortlich ist bzw. an wen der Abschluss der Realisierung der einzelnen Maßnahmen zu melden ist. Die Meldungen laufen beim ISB zusammen, der kontinuierlich über den Fortschritt der Realisierung und die Ergebnisse informiert wird. Der ISB wiederum muss regelmäßig die Leitungsebene über den Fortschritt und die damit verbundene Absenkung vorhandener Risiken informieren.

Der Realisierungsplan sollte mindestens folgende Informationen umfassen:

» Beschreibung des Zielobjektes (Einsatzumfeld),

» Nummer bzw. Titel des betrachteten Bausteins,

» Titel bzw. Beschreibung der zu erfüllenden Anforderung

» Beschreibung der umzusetzenden Maßnahme bzw. Verweis auf die Beschreibung im Sicherheitskonzept,

» Terminplanung für die Umsetzung,

» falls vorhanden: Abhängigkeiten und Querbeziehungen zu anderen Maßnahmen,

» verfügbares Budget,

» Verantwortliche für die Umsetzung und

» Verantwortliche für die Überwachung der Realisierung.

Aktionspunkte zu Umsetzung der Sicherheitskonzeption

» Fehlende oder nur teilweise umgesetzte IT-Grundschutz-Anforderungen sowie ergänzende Sicherheitsmaßnahmen zusammenfassen

» Sicherheitsmaßnahmen formulieren, welche die Basisanforderungen erfüllen

» Sicherheitsmaßnahmen konsolidieren, das heißt, überflüssige Maßnahmen streichen, allgemeine Maßnahmen an die Gegebenheiten anpassen und alle Maßnahmen auf Eignung prüfen

» Einmalige und wiederkehrende Kosten und Aufwand für die umzusetzenden Maßnahmen ermitteln

» Geeignete Ersatzmaßnahmen für nicht finanzierbare oder nicht leistbare Maßnahmen ermitteln

» Entscheidung herbeiführen, welche Ressourcen für die Umsetzung der Maßnahmen eingesetzt werden sollen

» Gegebenenfalls Restrisiko aufzeigen und Entscheidung der Leitungsebene darüber einholen

» Umsetzungsreihenfolge für die Maßnahmen festlegen, begründen und dokumentieren

» Termine für die Umsetzung festlegen und Verantwortung zuweisen

» Verlauf der Umsetzung und Einhaltung der Termine überwachen

» Betroffene Mitarbeiter schulen und sensibilisieren

4 Informationssicherheit ist ein Prozess: Wie es weitergehen kann

4 Informationssicherheit ist ein Prozess: Wie es weitergehen kann

Mit der Umsetzung der Basis-Absicherung ist ein wichtiger erster Schritt geschafft worden, das Niveau der Informationssicherheit in der Institution maßgeblich zu steigern. Damit wurde auch das Managementsystem für Informationssicherheit auf eine erste solide Basis gebracht. Die ausgewählten Sicherheitsmaßnahmen müssen weiter umgesetzt und Vorgaben wie die Sicherheitsleitlinie fortlaufend aktualisiert werden, um den nun begonnenen Informationssicherheitsprozess aufrecht zu erhalten und kontinuierlich verbessern zu können. Dazu gehört auch, den IS-Prozess selbst regelmäßig auf seine Wirksamkeit und Effizienz hin zu überprüfen.

Eine regelmäßige Erfolgskontrolle und Bewertung des Prozesses sollte auch durch die Leitung erfolgen. Häufen sich zum Beispiel Sicherheitsvorfälle oder gibt es gravierende Änderungen bei den Rahmenbedingungen, so muss eine Überprüfung auch zwischen den Routineterminen durchgeführt werden. Alle Ergebnisse und Beschlüsse müssen nachvollziehbar dokumentiert werden. Es ist Aufgabe des ISB, diese Informationen zu sammeln, zu verarbeiten und die Leitung zu informieren.

Mit der Basis-Absicherung kann eine Institution das Informationssicherheitsniveau bereits auf ein gutes Level anheben. Bei diesem initialen Prozess sind in der Institution viele Aspekte betrachtet, Fachverantwortliche beteiligt und Mitarbeiter sensibilisiert worden. Dennoch ist die Informationssicherheit ein so vielschichtiges wie dynamisches Aufgabengebiet, dass die Basis-Absicherung lediglich ein erster Einstieg in die Auseinan-

dersetzung mit der Thematik sein kann: Im besten Fall setzt die Institution den Prozess mit den beiden weiteren Vorgehensweisen aus der IT-Grundschutz-Methodik fort.

Kern-Absicherung

Im Fokus der Kern-Absicherung stehen zunächst die besonders gefährdeten Geschäftsprozesse und Assets. Diese Vorgehensweise ist empfehlenswert, wenn für eine Institution folgende Punkte überwiegend zutreffen:

» Die Anzahl der Geschäftsprozesse mit deutlich erhöhtem Schutzbedarf ist überschaubar bzw. umfasst nur einen kleinen Anteil aller Geschäftsprozesse der Institution.

» Die Institution kann die Geschäftsprozesse, die ein deutlich erhöhtes Gefährdungspotential bezüglich der Informationssicherheit haben, zügig identifizieren und eindeutig abgrenzen.

» Die Institution besitzt eindeutig benennbare Assets, deren Diebstahl, Zerstörung oder Kompromittierung einen existenzbedrohenden Schaden für die Institution bedeuten würde (sogenannte Kronjuwelen). Diese sollen vorrangig geschützt werden.

» Kleinere Sicherheitsvorfälle, die Geld kosten oder anderweitig Schaden verursachen, aber keinen existenzbedrohenden Schaden verursachen, sind für die Institution akzeptabel.

Standard-Absicherung

Die Standard-Absicherung entspricht im Wesentlichen der klassischen IT-Grundschutz-Vorgehensweise. Mit der Standard-

Absicherung kann ein ISB die Assets und Prozesse einer Institution sowohl umfassend als auch in der Tiefe absichern. Eine Aufnahme des Sicherheitsprozesses mit der Standard-Absicherung ist empfehlenswert, wenn für die Institution die folgenden Punkte überwiegend zutreffen:

» Die Umsetzung von Informationssicherheit hat in der Institution bereits einen ausreichenden Reifegrad erreicht, so dass in wesentlichen Bereichen bereits Sicherheitsmaßnahmen vorhanden sind und keine grundlegende Erst-Absicherung mehr notwendig ist.

» Es besteht kein Handlungsbedarf, einzelne Geschäftsprozesse vordringlich abzusichern, die ein deutlich höheres Gefährdungspotential bezüglich der Informationssicherheit besitzen (siehe Kern-Absicherung).

» Die Institution hat keine Assets, deren Diebstahl, Zerstörung oder Kompromittierung einen unmittelbar existenzbedrohenden Schaden nach sich ziehen könnte und die daher vorrangig abgesichert werden sollten.

» Sicherheitsvorfälle, die wahrnehmbar die Aufgabenerfüllung beeinträchtigen, Geld kosten oder anderweitig erkennbaren Schaden verursachen, sind für die Institution nicht akzeptabel, auch wenn sie noch keinen existenzbedrohenden Schaden verursachen.

Die Standard-Absicherung stellt innerhalb der IT-Grundschutz-Methodik diejenige Vorgehensweise dar, die grundsätzlich angestrebt werden sollte, um alle Bereiche einer Institution angemessen und umfassend zu schützen.

Jede Institution liefert mit der Erhöhung ihres Informationssicherheitsniveaus einen wichtigen Baustein zur Verbesserung

der Cyber-Sicherheit in Deutschland. Je mehr Verantwortliche in Unternehmen und Behörden sich mit den elementar wichtigen Fragen zur Informationssicherheit sowie Maßnahmen zu Schutz und Abwehr befassen, desto mehr profitiert der Wirtschaftsstandort Deutschland insgesamt davon. Der IT-Grundschutz bietet mit den modernisierten Inhalten in den BSI-Standards und im IT-Grundschutz-Kompendium ein umfangreiches und praktikables Angebot für Unternehmen und Behörden jeder Größenordnung.

5 Anhang

5 Anhang

5.1 Das IT-Grundschutz-Kompendium – Wissenswertes auf einen Blick

Das IT-Grundschutz-Kompendium enthält die IT-Grundschutz-Bausteine, in denen unterschiedliche Themen der Informationssicherheit im Hinblick auf die jeweils spezifische Gefährdungslage sowie Sicherheitsanforderungen aufbereitet sind. Es wird als Nachfolger der bisherigen IT-Grundschutz-Kataloge jährlich in Form einer aktualisierten Edition online zur Verfügung gestellt.

Die IT-Grundschutz-Bausteine

Das IT-Grundschutz-Kompendium enthält für unterschiedliche Prozesse, Komponenten und IT-Systeme Erläuterungen zur Gefährdungslage, Sicherheitsanforderungen und weiterführende Informationen, die jeweils in einem Baustein zusammengefasst sind. Das Kompendium ist aufgrund der Baustein-Struktur modular aufgebaut und legt einen Fokus auf die Darstellung der wesentlichen Sicherheitsanforderungen in den Bausteinen. Ziel ist es, durch diese Struktur neue technische Entwicklungen und Versionswechsel zeitnah berücksichtigen zu können. Einzelne Bausteine können so zeitnah erweitert und aktualisiert werden. Die grundlegende Struktur der Bausteine sieht eine Unterteilung in prozess- und systemorientierte Bausteine vor, zudem sind sie nach Themen in ein Schichtenmodell einsortiert.

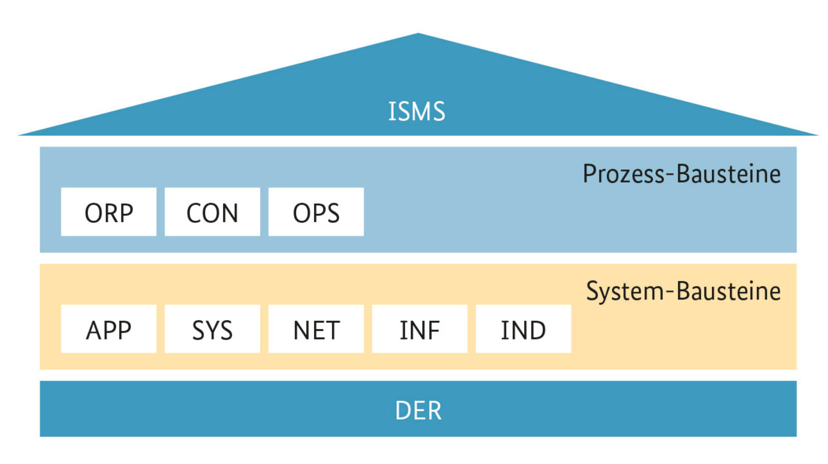


Abbildung 5: Das Schichtenmodell des IT-Grundschutz-Kompendiums

Prozess-Bausteine:

» Die Schicht ISMS enthält als Grundlage für alle weiteren Aktivitäten im Sicherheitsprozess den Baustein Sicherheitsmanagement.

» In der Schicht ORP finden sich Bausteine, die organisatorische und personelle Sicherheitsaspekte abdecken.

» Die Schicht CON enthält Bausteine, die sich mit Konzepten und Vorgehensweisen befassen.

» Die Schicht OPS umfasst alle Sicherheitsaspekte betrieblicher Art. Insbesondere sind dies die Sicherheitsaspekte des operativen IT-Betriebs, aber auch solche, die bei einem IT-Betrieb für Dritte zu beachten sind.

» In der Schicht DER finden sich alle Bausteine, die für die Überprüfung der umgesetzten Sicherheitsmaßnahmen und

insbesondere für die Detektion von Sicherheitsvorfällen sowie die geeigneten Reaktionen darauf relevant sind.

System-Bausteine:

» Die Schicht APP beschäftigt sich mit der Absicherung von Anwendungen und Diensten, unter anderem in den Bereichen Kommunikation, Verzeichnisdienste, Netzbasierte Dienste sowie Business- und Client-Anwendungen.

» Die Schicht SYS betrifft die einzelnen IT-Systeme des Informationsverbunds, die falls erforderlich in Gruppen zusammengefasst wurden.

» Die Schicht NET betrachtet die Vernetzungsaspekte, die sich nicht auf bestimmte IT-Systeme, sondern auf die Netzverbindungen und die Kommunikation beziehen.

» Die Schicht INF befasst sich mit den baulich-technischen Gegebenheiten, hier werden Aspekte der infrastrukturellen Sicherheit zusammengeführt.

» Die Schicht IND befasst sich mit Sicherheitsaspekten industrieller IT.

Die Aufteilung in Prozess- und System-Bausteine bietet den Vorteil, dass übergeordnete Aspekte und gemeinsame infrastrukturelle Fragestellungen getrennt von den IT-Systemen betrachtet werden können. Redundanzen werden vermieden, weil einzelne Aspekte nur jeweils einmal bearbeitet werden müssen und nicht für jedes IT-System noch einmal separat. Zudem können aufgrund der Aufteilung der Sicherheitsaspekte in Schichten Einzelaspekte in resultierenden Sicherheitskon-

zepten leichter aktualisiert und erweitert werden, ohne dass andere Schichten umfangreich betroffen sind.

Reihenfolge der Baustein-Umsetzung

Ziel der IT-Grundschutz-Methodik ist es, dass essentielle Sicherheitsanforderungen frühzeitig erfüllt und entsprechende Sicherheitsmaßnahmen umgesetzt werden. Daher wird für die Umsetzung der Bausteine folgende Reihenfolge vorgeschlagen:

» R1: Diese Bausteine sollten vorrangig umgesetzt werden, da sie die Grundlage für einen effektiven Sicherheitsprozess bilden.

» R2: Diese Bausteine sollten als nächstes umgesetzt werden, da sie in wesentlichen Teilen des Informationsverbundes für nachhaltige Sicherheit erforderlich sind.

» R3: Diese Bausteine werden zur Erreichung des angestrebten Sicherheitsniveaus ebenfalls benötigt und müssen umgesetzt werden, es wird aber empfohlen, diese erst nach den anderen Bausteinen zu betrachten.

Mit R1 sind diejenigen Bausteine gekennzeichnet, die notwendig sind, um ein grundlegendes Sicherheitsgerüst zu erreichen. Dabei handelt es sich um folgende Schichten:

» ISMS Sicherheitsmanagement

» ORP Organisation und Personal

» OPS.1.1 Kern-IT-Betrieb

Die Kennzeichnung der Reihenfolge stellt lediglich eine Empfehlung dar. Jede Institution kann eine abweichende, für ihre Belange sinnvolle Reihenfolge festlegen.

Gefährdungen

In jedem Baustein wird zunächst die spezifische Gefährdungslage für eine Thematik beschrieben. Dazu ergänzend befindet sich im jeweiligen Anhang eine Liste der elementaren Gefährdungen, die bei der Erstellung des Bausteins berücksichtigt wurden. Die Gefährdungsliste gehört zur ersten Stufe der vereinfachten Risikoanalyse für typische Umgebungen der Informationsverarbeitung und bildet die Grundlage, auf der das BSI spezifische Anforderungen zusammengestellt hat, deren Umsetzung ein angemessenes Niveau der Informationssicherheit in einer Institution gewährleisten kann. Der Vorteil ist, dass die Anwender bei typischen Szenarien keine aufwändigen oder weiterführenden Analysen durchführen müssen, um das für einen normalen Schutzbedarf notwendige Sicherheitsniveau zu erreichen. Es reicht aus, die für die betrachteten Geschäftsprozesse und ihrer notwendigen Ressourcen relevanten Bausteine zu identifizieren und die darin empfohlenen Anforderungen konsequent und vollständig umzusetzen.

Sicherheitsanforderungen

In jedem Baustein werden die Sicherheitsanforderungen, die für den Schutz des betrachteten Gegenstands relevant sind, aufgeführt. Sie beschreiben, was zu dessen Schutz zu tun ist. Die Anforderungen sind in drei Kategorien eingruppiert:

» **Basisanforderungen** müssen vorrangig erfüllt werden, da bei diesen Empfehlungen mit (relativ) geringem Aufwand

der größtmögliche Nutzen erzielt werden kann. Es handelt sich um uneingeschränkte Anforderungen. Die Basisanforderungen bilden die Grundlage für die Vorgehensweise „Basis-Absicherung“.

» **Standardanforderungen** bauen auf den Basisanforderungen auf und adressieren einen normalen Schutzbedarf. Sie sollten grundsätzlich erfüllt werden, aber nicht vorrangig. Die Ziele der Standardanforderungen müssen erreicht werden, um eine Standard-Absicherung zu erzielen. Es können sich aber durch die jeweiligen Rahmenbedingungen der Institution auch Gründe ergeben, warum eine Standardanforderung nicht wie beschrieben umgesetzt wird, sondern die Sicherheitsziele auf andere Weise erreicht werden. Wenn eine Standardanforderung durch andere Sicherheitsmaßnahmen erfüllt wird, müssen die dadurch entstehenden Auswirkungen sorgfältig abgewogen und geeignet dokumentiert werden.

» **Anforderungen für einen hohen Schutzbedarf** sind eine Auswahl von Vorschlägen für eine weitergehende Absicherung, die bei erhöhten Sicherheitsanforderungen oder unter bestimmten Rahmenbedingungen als Grundlage für die Erarbeitung geeigneter Anforderungen und Maßnahmen berücksichtigt werden können.

Umsetzungshinweise

Zu vielen Bausteinen des IT-Grundschutz-Kompendiums gibt es detaillierte Umsetzungshinweise. Diese beschreiben, wie die Anforderungen der Bausteine umgesetzt werden können und erläutern passende Sicherheitsmaßnahmen mit einer detaillierten Beschreibung. Die Sicherheitsmaßnahmen können als Grundlage für Sicherheitskonzeptionen verwendet werden, sie

sollten aber an die Rahmenbedingungen der jeweiligen Institution angepasst werden.

Die Umsetzungshinweise adressieren jeweils die Personengruppen, die für die Umsetzung der Baustein-Anforderungen zuständig sind, beispielsweise den IT-Betrieb oder die Haustechnik.

5.2 Literaturverzeichnis

[BSI1] Managementsysteme für Informationssicherheit (ISMS), BSI-Standard 200-1, Version 1.0, Oktober 2017, https://www.bsi.bund.de/grundschutz

[BSI2] IT-Grundschutz-Methodik, BSI-Standard 200-2, Version 1.0, Oktober 2017, https://www.bsi.bund.de/grundschutz

[BSI3] Risikoanalyse auf der Basis von IT-Grundschutz, BSI-Standard 200-3, Version 1.0, Oktober 2017, https://www.bsi.bund.de/grundschutz

[GSK] IT-Grundschutz-Kompendium – Standard-Sicherheitsmaßnahmen, BSI, jährlich neu, https://www.bsi.bund.de/grundschutz

5.3 Glossar

In diesem Glossar werden die wichtigsten Begriffe für Managementsysteme für Informationssicherheit (ISMS) aufgeführt. Ein hierzu ergänzendes Glossar zur Cyber-Sicherheit ist auf den Webseiten des BSI unter http://www.bsi.bund.de/cyberglossar zu finden.

Anforderungen bei erhöhtem Schutzbedarf
Siehe Sicherheitsanforderung.

Assets
Als Assets werden Bestände von Objekten bezeichnet, die für einen bestimmten Zweck, besonders zur Erreichung von Geschäftszielen, benötigt werden. Der englische Begriff „asset“ wird häufig mit „Wert“ übersetzt. „Wert“ ist allerdings im Deutschen ein mit vielen Bedeutungen belegter Begriff – von der gesellschaftlichen Bedeutung, die einer Sache zukommt, bis hin zur inneren Qualität eines Objekts. Im IT-Grundschutz wird der Begriff „Assets“ in der Bedeutung von „werthaltigen bzw. wertvollen Zielobjekten“ verwendet.

Basis-Absicherung
Die Basis-Absicherung ermöglicht es, als Einstieg in den IT-Grundschutz zunächst eine breite, grundlegende Erst-Absicherung über alle Geschäftsprozesse bzw. Fachverfahren einer Institution vorzunehmen.

Basis-Anforderung
Siehe Sicherheitsanforderung.

Bausteine
Das IT-Grundschutz-Kompendium enthält für unterschiedliche Vorgehensweisen, Komponenten und IT-Systeme Erläuterungen zur Gefährdungslage, Sicherheitsanforderungen und

weiterführende Informationen, die jeweils in einem Baustein zusammengefasst sind. Das Kompendium ist aufgrund der Baustein-Struktur modular aufgebaut und legt einen Fokus auf die Darstellung der wesentlichen Sicherheitsanforderungen in den Bausteinen. Die grundlegende Struktur der Bausteine sieht eine Unterteilung in prozess- und systemorientierte Bausteine vor, zudem sind sie nach Themen in ein Schichtenmodell einsortiert.

Cyber-Sicherheit
Cyber-Sicherheit befasst sich mit allen Aspekten der Sicherheit in der Informations- und Kommunikationstechnik. Das Aktionsfeld der Informationssicherheit wird dabei auf den gesamten Cyber-Raum ausgeweitet. Dieser umfasst sämtliche mit dem Internet und vergleichbaren Netzen verbundene Informationstechnik und schließt darauf basierende Kommunikation, Anwendungen, Prozesse und verarbeitete Informationen mit ein. Häufig wird bei der Betrachtung von Cyber-Sicherheit auch ein spezieller Fokus auf Angriffe aus dem Cyber-Raum gelegt.

Datenschutz
Datenschutz soll den Einzelnen davor schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinen Persönlichkeitsrechten beeinträchtigt wird. Mit Datenschutz wird daher der Schutz personenbezogener Daten vor etwaigem Missbrauch durch Dritte bezeichnet (nicht zu verwechseln mit Datensicherheit).
Für den Begriff „Datenschutz“ existieren zwei englische Übersetzungen: Dabei bezeichnet „data protection“ den Datenschutz als Rechtsbegriff. „Privacy“ zielt dagegen auf die gesellschaftliche Lebensweise ab (Schutz der Privatsphäre) und wird überwiegend im amerikanischen Sprachumfeld und mittlerweile auch im EU-Raum vermehrt genutzt.

Fachaufgabe
Fachaufgaben sind Aufgaben, die aus der Zweckbestimmung einer Institution bzw. deren Auftrag folgen. Als Fachaufgaben werden im IT-Grundschutz Geschäftsprozesse in Behörden bezeichnet.

Gefährdung
Eine Gefährdung ist eine Bedrohung, die konkret über eine Schwachstelle auf ein Objekt einwirkt. Eine Bedrohung wird somit erst durch eine vorhandene Schwachstelle zur Gefährdung für ein Objekt.

Geschäftsprozess
Ein Geschäftsprozess ist eine Menge logisch verknüpfter Einzeltätigkeiten (Aufgaben, Arbeitsabläufe), die ausgeführt werden, um ein bestimmtes geschäftliches oder betriebliches Ziel zu erreichen.

Grundwerte der Informationssicherheit
Der IT-Grundschutz betrachtet die drei Grundwerte der Informationssicherheit: Vertraulichkeit, Verfügbarkeit und Integrität. Jedem Anwender steht es natürlich frei, bei der Schutzbedarfsfeststellung weitere Grundwerte zu betrachten, wenn dies in seinem individuellem Anwendungsfall hilfreich ist. Weitere generische Oberbegriffe der Informationssicherheit sind zum Beispiel: Authentizität, Verbindlichkeit, Zuverlässigkeit, Nichtabstreitbarkeit.

Informationssicherheit
Informationssicherheit hat den Schutz von Informationen als Ziel. Dabei können Informationen sowohl auf Papier, in Rechnern oder auch in Köpfen gespeichert sein. IT-Sicherheit beschäftigt sich an erster Stelle mit dem Schutz elektronisch gespeicherter Informationen und deren Verarbeitung. Der Begriff „Informationssicherheit“ statt IT-Sicherheit ist daher

umfassender und wird zunehmend verwendet. Da aber in der Literatur noch überwiegend der Begriff „IT-Sicherheit“ zu finden ist, wird er auch in dieser sowie in anderen Publikationen des IT-Grundschutzes weiterhin verwendet, allerdings werden die Texte sukzessive stärker auf die Betrachtung von Informationssicherheit ausgerichtet.

Informationssicherheitsbeauftragter (ISB)
Ein Informationssicherheitsbeauftragter (kurz IS-Beauftragter oder ISB) ist für die operative Erfüllung der Aufgabe „Informationssicherheit“ zuständig. Andere Bezeichnungen sind CISO (Chief Information Security Officer) oder Informationssicherheitsmanager (ISM). Informationssicherheit umfasst den umfangreicheren Bereich des Schutzes von Informationen, zwar in und mit IT, aber auch ohne IT bzw. über IT hinaus. Somit ist IT-Sicherheit ein Teilbereich der Informationssicherheit und beschäftigt sich gezielt mit dem Schutz der eingesetzten IT. Neben dem ISB kann es auch einen dedizierten Beauftragten für IT-Sicherheit geben. Dieser ist dann typischerweise im IT-Bereich tätig, während der ISB unmittelbar der Leitungsebene zuarbeitet.

Informationssicherheitsmanagement (IS-Management)
Die Planungs-, Lenkungs- und Kontrollaufgabe, die erforderlich ist, um einen durchdachten und wirksamen Prozess zur Herstellung von Informationssicherheit aufzubauen und kontinuierlich umzusetzen, wird als Informationssicherheitsmanagement bezeichnet. Dabei handelt es sich um einen kontinuierlichen Prozess, dessen Strategien und Konzepte ständig auf ihre Leistungsfähigkeit und Wirksamkeit zu überprüfen und bei Bedarf fortzuschreiben sind.
Aus den gleichen Gründen, die oben für die Begriffe „Informationssicherheit“ und „IT-Sicherheit“ genannt sind, wird im IT-Grundschutz noch häufig der Begriff „IT-Sicherheitsmanagement“ verwendet.

Informationstechnik (IT)
Informationstechnik (IT) umfasst alle technischen Mittel, die der Verarbeitung oder Übertragung von Informationen dienen. Zur Verarbeitung von Informationen gehören Erhebung, Erfassung, Nutzung, Speicherung, Übermittlung, programmgesteuerte Verarbeitung, interne Darstellung und die Ausgabe von Informationen.

Informationsverbund
Unter einem Informationsverbund (oder auch IT-Verbund) ist die Gesamtheit von infrastrukturellen, organisatorischen, personellen und technischen Objekten zu verstehen, die der Aufgabenerfüllung in einem bestimmten Anwendungsbereich der Informationsverarbeitung dienen. Ein Informationsverbund kann dabei als Ausprägung die gesamte Institution oder auch einzelne Bereiche, die durch organisatorische Strukturen (z. B. Abteilungen) oder gemeinsame Geschäftsprozesse bzw. Anwendungen (z. B. Personalinformationssystem) gegliedert sind, umfassen.

Institutionen
Mit dem Begriff Institutionen werden in diesem Dokument Unternehmen, Behörden und sonstige öffentliche oder private Organisationen bezeichnet.

Integrität
Integrität bezeichnet die Sicherstellung der Korrektheit (Unversehrtheit) von Daten und der korrekten Funktionsweise von Systemen. Wenn der Begriff Integrität auf „Daten“ angewendet wird, drückt er aus, dass die Daten vollständig und unverändert sind. In der Informationstechnik wird er in der Regel aber weiter gefasst und auf „Informationen“ angewendet. Der Begriff „Information“ wird dabei für „Daten“ verwendet, denen je nach Zusammenhang bestimmte Attribute wie z. B. Autor oder Zeitpunkt der Erstellung zugeordnet werden können. Der Verlust

der Integrität von Informationen kann daher bedeuten, dass diese unerlaubt verändert, Angaben zum Autor verfälscht oder Zeitangaben zur Erstellung manipuliert wurden.

IT-Grundschutz-Check
Der Begriff bezeichnet im IT-Grundschutz die Überprüfung, ob die nach IT-Grundschutz empfohlenen Anforderungen in einer Institution bereits erfüllt sind und welche grundlegenden Sicherheitsanforderungen noch fehlen (früher: Basis-Sicherheitscheck).

IT-Grundschutz-Kompendium
Die Bausteine des IT-Grundschutzes sind im IT-Grundschutz-Kompendium zusammengefasst. Es stellt den Nachfolger der bis zur 15. Ergänzungslieferung verfügbaren IT-Grundschutz-Kataloge dar.

IT-Sicherheitsbeauftragter (IT-SiBe)
Person mit Fachkompetenz zur IT-Sicherheit, die für Aspekte rund um die IT-Sicherheit zuständig ist, in enger Abstimmung mit dem IT-Betrieb. Die Rolle des Verantwortlichen für Informationssicherheit wird je nach Art und Ausrichtung der Institution anders genannt. Im IT-Grundschutz wird die Bezeichnung Informationssicherheitsbeauftragter (ISB) verwendet.

Kern-Absicherung
Im Fokus der Kern-Absicherung stehen zunächst die besonders gefährdeten Geschäftsprozesse und Assets.

Kronjuwelen
Als Kronjuwelen werden solche Assets bezeichnet, deren Diebstahl, Zerstörung oder Kompromittierung einen existenzbedrohenden Schaden für die Institution bedeuten würde.

Leitlinie zur Informationssicherheit
Die Leitlinie ist ein zentrales Dokument für die Informationssicherheit einer Institution. In ihr wird beschrieben, für welche Zwecke, mit welchen Mitteln und mit welchen Strukturen Informationssicherheit innerhalb der Institution hergestellt werden soll. Sie beinhaltet die von der Institution angestrebten Informationssicherheitsziele sowie die verfolgte Sicherheitsstrategie. Die Sicherheitsleitlinie beschreibt damit auch über die Sicherheitsziele das angestrebte Sicherheitsniveau in einer Behörde oder einem Unternehmen.

Risiko
Risiko wird häufig definiert als die Kombination (also dem Produkt) aus der Häufigkeit, mit der ein Schaden auftritt und dem Ausmaß dieses Schadens. Der Schaden wird häufig als Differenz zwischen einem geplanten und ungeplanten Ergebnis dargestellt. Risiko ist eine spezielle Form der Unsicherheit oder besser Unwägbarkeit.
In der ISO 31000 wird Risiko auch als das Ergebnis von Unwägbarkeiten auf Zielobjekte definiert. In diesem Sinne wird daher auch von Konsequenzen statt von Schaden gesprochen, wenn Ereignisse anders eintreten als erwartet. Hierbei kann eine Konsequenz negativ (Schaden) oder positiv (Chance) sein. Die obige Definition hat sich allerdings als gängiger in der Praxis durchgesetzt.
Im Unterschied zu „Gefährdung“ umfasst der Begriff „Risiko“ bereits eine Bewertung, inwieweit ein bestimmtes Schadensszenario im jeweils vorliegenden Fall relevant ist.

Risikoanalyse
Als Risikoanalyse wird der komplette Prozess bezeichnet, um Risiken zu beurteilen (identifizieren, einschätzen und bewerten) sowie zu behandeln. Risikoanalyse bezeichnet nach den einschlägigen ISO-Normen ISO 31000 und ISO 27005 nur einen

Schritt im Rahmen der Risikobeurteilung, die aus den folgenden Schritten besteht:
» Identifikation von Risiken (Risk Identification)
» Analyse von Risiken (Risk Analysis)
» Evaluation oder Bewertung von Risiken (Risk Evaluation)
Im deutschen Sprachgebrauch hat sich allerdings der Begriff Risikoanalyse für den kompletten Prozess der Risikobeurteilung und Risikobehandlung etabliert. Daher wird auch in diesem Dokument weiter der Begriff Risikoanalyse für den umfassenden Prozess benutzt.

Risikomanagement
Als Risikomanagement werden alle Aktivitäten mit Bezug auf die strategische und operative Behandlung von Risiken bezeichnet, also alle Tätigkeiten, um Risiken für eine Institution zu identifizieren, zu steuern und zu kontrollieren.
Das strategische Risikomanagement beschreibt die wesentlichen Rahmenbedingungen, wie die Behandlung von Risiken innerhalb einer Institution, die Kultur zum Umgang mit Risiken und die Methodik ausgestaltet sind. Diese Grundsätze für die Behandlung von Risiken innerhalb eines ISMS müssen mit den Rahmenbedingungen des organisationsweiten Risikomanagements übereinstimmen bzw. aufeinander abgestimmt sein.
Die Rahmenbedingungen des operativen Risikomanagements umfassen den Regelprozess aus
» Identifikation von Risiken,
» Einschätzung und Bewertung von Risiken,
» Behandlung von Risiken,
» Überwachung von Risiken und
» Risikokommunikation.

Schaden/Konsequenz
Eine Abweichung von einem erwarteten Ergebnis führt zu einer Konsequenz (häufig „Schaden“ genannt). Hierbei kann es

sich grundsätzlich um eine positive oder negative Abweichung handeln.
Eine positive Konsequenz/positiver Schaden im Sinne der Chancen- und Risikoanalyse wird auch als Chance bezeichnet. Meistens werden in der Risikoanalyse jedoch die negativen Konsequenzen, also die Schäden, betrachtet.
Das Ausmaß eines Schadens wird als Schadenshöhe definiert und kann als bezifferbar oder nicht direkt bezifferbar betitelt werden. Die bezifferbaren Schäden können in der Regel mit direkten Aufwänden (z. B. finanzieller Art) dargestellt werden. Zu den nicht direkt bezifferbaren Schäden gehören z. B. Imageschäden oder Opportunitätskosten. Bei diesen lässt sich die tatsächliche Schadenshöhe häufig nur vermuten oder schätzen. Alle Angaben werden in der Regel aufgrund von Erfahrungs- oder Branchenwerten in Kategorien klassifiziert.

Schwachstelle
Eine Schwachstelle ist ein sicherheitsrelevanter Fehler eines IT-Systems oder einer Institution. Ursachen können in der Konzeption, den verwendeten Algorithmen, der Implementation, der Konfiguration, dem Betrieb sowie der Organisation liegen. Eine Schwachstelle kann dazu führen, dass eine Bedrohung wirksam wird und eine Institution oder ein System geschädigt wird. Durch eine Schwachstelle wird ein Objekt (eine Institution oder ein System) anfällig für Bedrohungen.

Sicherheitsanforderung
Als Sicherheitsanforderungen werden Anforderungen für den organisatorischen, personellen, infrastrukturellen und technischen Bereich bezeichnet, deren Erfüllung zur Erhöhung der Informationssicherheit notwendig ist bzw. dazu beiträgt. Eine Sicherheitsanforderung beschreibt also, was getan werden muss, um ein bestimmtes Niveau bezüglich der Informationssicherheit zu erreichen. Wie die Anforderungen im konkreten Fall erfüllt werden können, ist in entsprechenden Sicherheits-

maßnahmen beschrieben (siehe dort). Im englischen Sprachraum wird für Sicherheitsanforderungen häufig der Begriff „control“ verwendet.
Der IT-Grundschutz unterscheidet zwischen Basisanforderungen, Standardanforderungen und Anforderungen bei erhöhtem Schutzbedarf. Basisanforderungen sind fundamental und stets umzusetzen, sofern nicht gravierende Gründe dagegen sprechen. Standardanforderungen sind für den normalen Schutzbedarf grundsätzlich umzusetzen, sofern sie nicht durch mindestens gleichwertige Alternativen oder die bewusste Akzeptanz des Restrisikos ersetzt werden. Anforderungen bei erhöhtem Schutzbedarf sind exemplarische Vorschläge, was bei entsprechendem Schutzbedarf zur Absicherung sinnvoll umzusetzen ist.

Sicherheitskonzept
Ein Sicherheitskonzept dient zur Umsetzung der Sicherheitsstrategie und beschreibt die geplante Vorgehensweise, um die gesetzten Sicherheitsziele einer Institution zu erreichen. Das Sicherheitskonzept ist das zentrale Dokument im Sicherheitsprozess eines Unternehmens bzw. einer Behörde. Jede konkrete Sicherheitsmaßnahme muss sich letztlich darauf zurückführen lassen.

Sicherheitskonzeption
Die Erstellung einer Sicherheitskonzeption ist eine der zentralen Aufgaben des Informationssicherheitsmanagements. Aufbauend auf den Ergebnissen von Strukturanalyse und Schutzbedarfsfeststellung werden hier die erforderlichen Sicherheitsmaßnahmen identifiziert und im Sicherheitskonzept dokumentiert.

Sicherheitsmaßnahme
Mit Sicherheitsmaßnahme (kurz Maßnahme) werden alle Aktionen bezeichnet, die dazu dienen, um Sicherheitsrisiken

zu steuern und um diesen entgegenzuwirken. Dies schließt sowohl organisatorische, als auch personelle, technische oder infrastrukturelle Sicherheitsmaßnahmen ein. Sicherheitsmaßnahmen dienen zur Erfüllung von Sicherheitsanforderungen (siehe dort). Synonym werden auch die Begriffe Sicherheitsvorkehrung oder Schutzmaßnahme benutzt. Als englische Übersetzung wurde „safeguard", „security measure" oder „measure" gewählt.

Sicherheitsrichtlinie
In einer Sicherheitsrichtlinie werden Schutzziele und allgemeine Sicherheitsanforderung im Sinne offizieller Vorgaben eines Unternehmens oder einer Behörde formuliert. Detaillierte Sicherheitsmaßnahmen sind in einem umfangreicheren Sicherheitskonzept enthalten.

Standard-Absicherung
Die Standard-Absicherung entspricht im Wesentlichen der klassischen IT-Grundschutz-Vorgehensweise. Mit der Standard-Absicherung kann ein ISB die Assets und Prozesse einer Institution sowohl umfassend als auch in der Tiefe absichern.

Standardanforderung
Siehe Sicherheitsanforderung.

Strukturanalyse
In einer Strukturanalyse werden die erforderlichen Informationen über den ausgewählten Informationsverbund, die Anwendungen, IT-Systeme, Netze, Räume, Gebäude und Verbindungen erfasst und so aufbereitet, dass sie die weiteren Schritte gemäß IT-Grundschutz unterstützen.

Verfügbarkeit
Die Verfügbarkeit von Dienstleistungen, Funktionen eines IT-Systems, IT-Anwendungen oder IT-Netzen oder auch von

Informationen ist vorhanden, wenn diese von den Anwendern stets wie vorgesehen genutzt werden können.

Vertraulichkeit
Vertraulichkeit ist der Schutz vor unbefugter Preisgabe von Informationen. Vertrauliche Daten und Informationen dürfen ausschließlich Befugten in der zulässigen Weise zugänglich sein.

Wert
Werte (engl. „assets“) sind alles, was wichtig für eine Institution ist (Vermögen, Wissen, Gegenstände, Gesundheit).

Zielobjekte
Zielobjekte sind Teile des Informationsverbunds, denen im Rahmen der Modellierung ein oder mehrere Bausteine aus dem IT-Grundschutz-Kompendium zugeordnet werden können. Zielobjekte können dabei physische Objekte sein, wie beispielsweise Netze oder IT-Systeme. Häufig sind Zielobjekte jedoch logische Objekte, wie beispielsweise Organisationseinheiten, Anwendungen oder der gesamte Informationsverbund.

Impressum

Herausgeber
Bundesamt für Sicherheit in der Informationstechnik – BSI
Godesberger Allee 185–189
53175 Bonn
E-Mail: grundschutz@bsi.bund.de
Internet: www.bsi.bund.de/grundschutz

Bezugsquelle
Bundesamt für Sicherheit in der Informationstechnik – BSI
Godesberger Allee 185–189
53175 Bonn
E-Mail: bsi@bsi.bund.de
Internet: www.bsi.bund.de
Telefon +49 (0) 22899 9582-0
Telefax +49 (0) 22899 9582-5400

Stand
Oktober 2017

Druck
Druck- und Verlagshaus Zarbock GmbH & Co. KG
Sontraer Straße 6
63086 Frankfurt am Main
Internet: www.zarbock.de

Texte und Redaktion
Bundesamt für Sicherheit in der Informationstechnik – BSI

Bildnachweis
Titelbild: kran 77, Fotolia

Artikelnummer
BSI-Bro17/CK02

www.bsi.bund.de/grundschutz